



Odbor za građanske slobode, pravosuđe i unutarnje poslove

2020/0359(COD)

15.10.2021

MIŠLJENJE

Odbora za građanske slobode, pravosuđe i unutarnje poslove

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Izvjestitelj za mišljenje: Lukas Mandl

(*)

Pridruženi odbor – članak 57. Poslovnika

PA_Legam

KRATKO OBRAZLOŽENJE

Prijedlog direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS2)¹ dio je šireg skupa inicijativa na razini Unije kojima se nastoji povećati otpornost javnih i privatnih subjekata na prijetnje. Cilj je prijedloga ukloniti nedostatke postojećeg zakonodavstva i omogućiti subjektima obuhvaćenima njegovim područjem primjene da bolje odgovore na nove izazove koje je Komisija utvrdila u svojoj procjeni učinka, koja je obuhvaćala opsežno savjetovanje s dionicima. Ti izazovi posebno uključuju rastuću digitalizaciju unutarnjeg tržišta i sve veće kibersigurnosne prijetnje.

Pravna je osnova Prijedloga članak 114. UFEU-a, to jest unutarnje tržište. Međutim, iz perspektive odbora LIBE važno je naglasiti da mjere uvedene za mrežne i informacijske sustave Direktivom NIS2 ne služe samo osiguravanju pravilnog funkcioniranja unutarnjeg tržišta. **Direktivom bi se trebalo pridonijeti i sigurnosti Unije u cjelini**, među ostalim izbjegavanjem različitih osjetljivosti na kibersigurnosne rizike među državama članicama.

U tu je svrhu ključno **ukloniti postojeće razlike među državama članicama** koje proizlaze iz različitih tumačenja prava u državama članicama. Zbog toga izvjestitelj pozdravlja jedinstveni uvjet utvrđen Uredbom za utvrđivanje subjekata koji su obuhvaćeni područjem primjene Direktive. Daju se dodatni prijedlozi kako bi se spriječile razlike u provedbi, posebno kako bi se Komisiju obvezalo da izda smjernice o provedbi *lex specialista* i kriterijima koji se primjenjuju na MSP-ove (čime bi se također trebala osigurati pravna jasnoća i izbjegći nepotrebno opterećenje) te kako bi se od skupine za suradnju zatražilo da dodatno odredi netehničke čimbenike koje treba uzeti u obzir u procjenama rizika u lancu opskrbe. Nadalje, naglašava se da se suradnja među nadležnim tijelima mora odvijati i unutar država članica i *među* njima, u stvarnom vremenu.

U nacrtu izvješća uzima se u obzir i niz **preporuka koje je EDPS** iznio u svojem mišljenju o strategiji za kibersigurnost i Direktivi NIS 2.0². Što je najvažnije, u uvodnim izjavama i u izvršnom dijelu teksta pojašnjeno je da se nijednom obradom osobnih podataka na temelju Direktive NIS2 ne dovode u pitanje Uredba (EU) 2016/679 (Opća uredba o zaštiti podataka)³ i Direktiva 2002/58/EZ⁴ (e-privatnost). S obzirom na uže područje primjene pojma „sigurnost mreža i informacijskih sustava“ (obuhvaća samo zaštitu tehnologije) u usporedbi s „kibersigurnosti“ (obuhvaća i aktivnosti za zaštitu korisnika), prethodni izraz upotrebljava se samo ako je kontekst isključivo tehničke prirode. Kad je riječ o nazivima domena i registracijskim podacima, predlažu se pojašnjenja u pogledu 1) pravne osnove za objavu „relevantnih informacija“ za potrebe identifikacije i kontaktiranja, 2) kategorija podataka o

¹ 2020/0359(COD).

² Mišljenje br. 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

³ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Tekst značajan za EGP), *SL L 119, 4.5.2016., str. 1.-88.*

⁴ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), *SL L 201, 31.7.2002., str. 37.-47.*

registraciji domene koje podliježu objavi (na temelju preporuke ICANN-a) i 3) subjekata koji bi mogli biti „zakoniti tražitelji pristupa”. U pravnom je tekstu navedeno i da prijedlog ne utječe na dodjelu nadležnosti i kompetencije nadzornih tijela za zaštitu podataka u skladu s Općom uredbom o zaštiti podataka. Naposljetku, pruža se sveobuhvatnija pravna osnova za suradnju i razmjenu relevantnih informacija između nadležnih tijela u skladu s Prijedlogom i drugih relevantnih nadzornih tijela, posebno nadzornih tijela u skladu s Općom uredbom o zaštiti podataka.

Ostale izmjene koje je izvjestitelj odbora LIBE uveo u prijedlog Komisije odnose se na sljedeće:

- Kako bi se osigurala usklađenost između Direktive NIS2 i predložene Direktive o otpornosti ključnih subjekata⁵, tekst nekih odredbi uskladen je s tekstrom prijedloga Direktive o otpornosti ključnih subjekata. U skladu sa sličnom izmjenom predviđenom za Direktivu o otpornosti ključnih subjekata kojom bi se trebali obuhvatiti isti sektori kao i Direktivom NIS2, predlaže se da područje primjene proširi na „proizvodnju, preradu i distribuciju hrane”.
- Kad je riječ o osobnim podacima, pojašnjeno je da pregledavanje mreža i informacijskih sustava koje provode CSIRT-ovi ne bi trebalo biti samo u skladu s Uredbom (EU) 2016/679 (Opća uredba o zaštiti podataka)⁶, nego i s Direktivom 2002/58/EZ⁷ (e-privatnost). Međunarodni prijenosi osobnih podataka na temelju ove Direktive trebali bi biti u skladu s poglavljem V. Opće uredbe o zaštiti podataka.
- Skupina za suradnju trebala bi se sastajati dvaput, a ne jednom godišnje kako bi razmotrila najnovija kretanja u području kibersigurnosti. Europski odbor za zaštitu podataka trebao bi sudjelovati na sastancima skupine za suradnju u ulozi promatrača.
- ENISA bi trebala izdavati godišnja, a ne dvogodišnja izvješća o stanju kibersigurnosti u Uniji. Izvješćem bi se trebao uzeti u obzir i učinak kiberincidenta na zaštitu osobnih podataka u Uniji.
- Rok za obavljanje o incidentima usklađen je s rokom za obavljanje o povredama u skladu s Općom uredbom o zaštiti podataka te iznosi 72 sata.
- Iako bi obavljanje o stvarnim kiberincidentima koje provode ključni i važni subjekti doista trebalo biti obvezno, obavljanje o kiberprijetnjama trebalo bi biti dobrovoljno kako bi se ograničilo administrativno opterećenje i izbjeglo prekomjerno prijavljivanje. Incident se smatra značajnim ako se njime uzrokuje stvarna šteta i utječe na druge fizičke i pravne osobe, a ne ako postoji tek „mogućnost“ za takvu štetu ili učinak.
- Okolnosti koje treba uzeti u obzir pri odlučivanju o sankcijama zbog povrede pravila o kibersigurnosti uskladene su s Općom uredbom o zaštiti podataka. Budući da bi to bilo protivno trenutačnoj praksi odgovornosti u pravu Unije, ne bi trebalo biti moguće nametnuti privremenu zabranu fizičkim osobama da obavljaju upravljačke funkcije.

⁵ 2020/0365(COD).

⁶ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Tekst značajan za EGP), *SL L 119, 4.5.2016.*, str. 1.-88.

⁷ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), *SL L 201, 31.7.2002.*, str. 37.-47.

- Kako bi se izbjegla šteta za ugled, subjekti ne bi trebali biti obvezni objaviti aspekte neusklađenosti sa zahtjevima iz ove Direktive ili identitet fizičkih ili pravnih osoba odgovornih za kršenje.

AMANDMANI

Odbor za građanske slobode, pravosuđe i unutarnje poslove pozive Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1

Prijedlog direktive Uvodna izjava 1.

Tekst koji je predložila Komisija

(1) Cilj Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća¹¹ bio je izgradnja kibersigurnosnih kapaciteta širom Unije, ublažavanje prijetnji mrežnim i informacijskim sustavima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju kiberincidenata, što pridonosi učinkovitom funkciranju gospodarstva i društva Unije.

¹¹ Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194/1, 19.7.2016., str. 1.).

Izmjena

(1) Cilj Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća¹¹ bio je izgradnja kibersigurnosnih kapaciteta širom Unije, ublažavanje prijetnji mrežnim i informacijskim sustavima koji se upotrebljavaju za pružanje osnovnih usluga u ključnim sektorima i osiguravanje kontinuiteta takvih usluga u slučaju kiberincidenata, što pridonosi **sigurnosti** Unije **i** učinkovitom funkciranju **njezina** gospodarstva i društva.

¹¹ Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194/1, 19.7.2016., str. 1.).

Amandman 2

Prijedlog direktive Uvodna izjava 2.

Tekst koji je predložila Komisija

(2) Od stupanja na snagu Direktive (EU) 2016/1148 ostvaren je znatan napredak u povećanju Unijine razine

Izmjena

(2) Od stupanja na snagu Direktive (EU) 2016/1148 ostvaren je znatan napredak u povećanju Unijine razine

otpornosti u području kibersigurnosti. Preispitivanje te direktive pokazalo je da je bila katalizator za institucionalni i regulatorni pristup kibersigurnosti u Uniji i omogućila bitnu promjenu načina razmišljanja. Njome je osiguran dovršetak nacionalnih okvira utvrđivanjem nacionalnih strategija za kibersigurnost, uspostavom nacionalnih kapaciteta i provedbom regulatornih mjera kojima su obuhvaćeni ključna infrastruktura i akteri koje je utvrdila svaka država članica. Pridonijela je i suradnji na razini Unije osnivanjem skupine za suradnju¹² i mreže nacionalnih timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova“)¹³. Neovisno o tim postignućima, preispitivanjem Direktive (EU) 2016/1148 otkriveni su bitni nedostaci zbog kojih se njome ne mogu učinkovito svladati aktualni i novi izazovi u području kibersigurnosti.

otpornosti u području kibersigurnosti. Preispitivanje te direktive pokazalo je da je bila katalizator za institucionalni i regulatorni pristup kibersigurnosti u Uniji i omogućila bitnu promjenu načina razmišljanja. Njome je osiguran dovršetak nacionalnih okvira utvrđivanjem nacionalnih strategija za kibersigurnost, uspostavom nacionalnih kapaciteta i provedbom regulatornih mjera kojima su obuhvaćeni ključna infrastruktura i akteri koje je utvrdila svaka država članica. Pridonijela je i suradnji na razini Unije osnivanjem skupine za suradnju i mreže nacionalnih timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova“). Neovisno o tim postignućima, preispitivanjem Direktive (EU) 2016/1148 otkriveni su bitni nedostaci zbog kojih se njome ne mogu učinkovito svladati aktualni i novi izazovi u području kibersigurnosti. *Osim toga, širenjem internetskih aktivnosti u kontekstu pandemije bolesti COVID-19 istaknuta je važnost kibersigurnosti, koja je ključna za povjerenje građana EU-a u inovacije i povezivost, kao i opsežnog obrazovanja i osposobljavanja u tom području. Komisija bi stoga trebala podupirati države članice u osmišljavanju obrazovnih programa o kibersigurnosti kako bi se važnim i ključnim subjektima omogućilo zapošljavanje stručnjaka za kibersigurnost koji im omogućuju da ispunе obveze koje proizlaze iz ove Direktive.*

¹² Članak 11. Direktive (EU) 2016/1148.

¹³ Članak 12. Direktive (EU) 2016/1148.

¹² Članak 11. Direktive (EU) 2016/1148.

¹³ Članak 12. Direktive (EU) 2016/1148.

Amandman 3

Prijedlog direktive Uvodna izjava 3.

Tekst koji je predložila Komisija

(3) Mrežni i informacijski sustavi razvili su se u okosnicu svakodnevnog života uz brzu digitalnu transformaciju i međupovezanost društva, među ostalim u prekograničnim razmjenama. Taj je razvoj doveo do povećanja kibersigurnosnih prijetnji te time i novih izazova koji zahtijevaju prilagođene, koordinirane i inovativne odgovore u svim državama članicama. Kibersigurnosni incidenti sve su brojniji, sofisticirаниji, učestaliji, većih razmjera i utjecaja te predstavljaju veliku prijetnju funkciranju mrežnih i informacijskih sustava. Zbog toga kiberincidenti mogu ugroziti obavljanje gospodarskih djelatnosti na unutarnjem tržištu, uzrokovati finansijske gubitke, narušiti povjerenje korisnika **i** nanijeti veliku štetu gospodarstvu i **društvu** Unije. Pripravnost i učinkovitost u području kibersigurnosti sada su važnije nego ikad za pravilno funkciranje unutarnjeg tržišta.

Izmjena

(3) Mrežni i informacijski sustavi razvili su se u okosnicu svakodnevnog života uz brzu digitalnu transformaciju i međupovezanost društva, među ostalim u prekograničnim razmjenama. Taj je razvoj doveo do povećanja kibersigurnosnih prijetnji te time i novih izazova koji zahtijevaju prilagođene, koordinirane i inovativne odgovore u svim državama članicama. Kibersigurnosni incidenti sve su brojniji, sofisticirаниji, učestaliji, većih razmjera i utjecaja te predstavljaju veliku prijetnju funkciranju mrežnih i informacijskih sustava. Zbog toga kiberincidenti mogu ugroziti obavljanje gospodarskih djelatnosti na unutarnjem tržištu, uzrokovati finansijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije, **funkcioniranju naše demokracije i vrijednostima i slobodi na kojima se temelji naše društvo**. Pripravnost i učinkovitost u području kibersigurnosti sada su važnije nego ikad za **sigurnost Unije i** pravilno funkciranje unutarnjeg tržišta s **obzirom na digitalnu transformaciju svakodnevnih aktivnosti diljem Unije**. Za to je potrebna tješnja suradnja tijela unutar država članica i među njima, kao i suradnja između nacionalnih tijela i odgovornih tijela Unije.

Amandman 4

**Prijedlog direktive
Uvodna izjava 5.**

Tekst koji je predložila Komisija

(5) Sve one dovode do rascjepkanosti unutarnjeg tržišta i mogu štetno utjecati na njegovo funkciranje, posebno na prekogranično pružanje usluga i razinu otpornosti u području kibersigurnosti zbog

Izmjena

(5) Sve one dovode do rascjepkanosti unutarnjeg tržišta i mogu štetno utjecati na njegovo funkciranje, posebno na prekogranično pružanje usluga i razinu otpornosti u području kibersigurnosti zbog

primjene različitih normi. Cilj je ove Direktive ukloniti velike razlike među državama članicama, posebno određivanjem minimalnih pravila o funkciranju koordiniranog regulatornog okvira, utvrđivanjem mehanizama za djelotvornu suradnju nadležnih tijela u svakoj državi članici, ažuriranjem popisa sektora i djelatnosti koji podliježu kibersigurnosnim obvezama te osiguravanjem djelotvornih pravnih lijekova i sankcija ključnih za učinkovito izvršavanje tih obveza. Stoga bi Direktivu (EU) 2016/1148 trebalo staviti izvan snage i zamijeniti ovom Direktivom.

primjene različitih normi. *Naposljetku, te razlike mogu dovesti do veće osjetljivosti nekih država članica na kibersigurnosne prijetnje, s mogućim učincima prelijevanja diljem Unije, kako u pogledu njezina unutarnjeg tržišta tako i u pogledu njezine opće sigurnosti.* Cilj je ove Direktive ukloniti velike razlike među državama članicama, posebno određivanjem minimalnih pravila o funkciranju koordiniranog regulatornog okvira, utvrđivanjem mehanizama za djelotvornu suradnju *u stvarnom vremenu* nadležnih tijela u svakoj državi članici, *kao i među nadležnim tijelima država članica*, ažuriranjem popisa sektora i djelatnosti koji podliježu kibersigurnosnim obvezama te osiguravanjem djelotvornih pravnih lijekova i sankcija ključnih za učinkovito izvršavanje tih obveza. Stoga bi Direktivu (EU) 2016/1148 trebalo staviti izvan snage i zamijeniti ovom Direktivom.

Amandman 5

Prijedlog direktive Uvodna izjava 6.

Tekst koji je predložila Komisija

(6) Ova Direktiva ne utječe na mogućnost država članica da poduzmu potrebne mjere za osiguravanje zaštite osnovnih interesa svoje sigurnosti, zaštitu javnog poretku i javne sigurnosti te omogućivanje istrage, otkrivanja i progona kaznenih djela, u skladu s pravom Unije. U skladu s člankom 346. UFEU-a nijedna država članica nije obvezna davati informacije ako smatra da bi njihovo otkrivanje bilo suprotno osnovnim interesima njezine javne sigurnosti. U tom su kontekstu relevantni nacionalna pravila i pravila Unije za zaštitu klasificiranih podataka, sporazumi o povjerljivosti podataka i neformalni sporazumi o povjerljivosti podataka kao što je Protokol

Izmjena

(6) Ova Direktiva ne utječe na mogućnost država članica da poduzmu potrebne mjere za osiguravanje zaštite osnovnih interesa svoje *nacionalne* sigurnosti, zaštitu javnog poretku i javne sigurnosti te omogućivanje *sprečavanja*, istrage, otkrivanja i progona kaznenih djela, u skladu s pravom Unije. U skladu s člankom 346. UFEU-a nijedna država članica nije obvezna davati informacije ako smatra da bi njihovo otkrivanje bilo suprotno osnovnim interesima njezine javne sigurnosti. U tom su kontekstu relevantni nacionalna pravila i pravila Unije za zaštitu klasificiranih podataka, sporazumi o povjerljivosti podataka i neformalni sporazumi o povjerljivosti

o semaforu¹⁴.

¹⁴ Protokol o semaforu instrument je kojim netko tko dijeli informacije obavješćuje primatelje o svim ograničenjima u dalnjem širenju tih informacija. Upotrebljavaju ga gotovo sve zajednice CSIRT-ova i neki centri za analizu i razmjenu informacija (ISAC).

podataka kao što je Protokol o semaforu¹⁴.

¹⁴ Protokol o semaforu instrument je kojim netko tko dijeli informacije obavješćuje primatelje o svim ograničenjima u dalnjem širenju tih informacija. Upotrebljavaju ga gotovo sve zajednice CSIRT-ova i neki centri za analizu i razmjenu informacija (ISAC).

Amandman 6

Prijedlog direktive Uvodna izjava 8.

Tekst koji je predložila Komisija

(8) ***U*** skladu s Direktivom (EU) 2016/1148, države članice bile su odgovorne za utvrđivanje subjekata koji ispunjavaju kriterije na temelju kojih ih se smatralo operatorima ključnih usluga („postupak utvrđivanja”). ***Kako bi se uklonile velike razlike*** među državama članicama u tom pogledu ***i osigurala pravna sigurnost za zahtjeve za upravljanje rizicima i obveze izvješćivanja za sve relevantne subjekte***, trebalo bi uspostaviti jedinstveni kriterij za određivanje subjekata obuhvaćenih područjem primjene ove Direktive. Taj bi se kriterij trebao sastojati od primjene pravila o veličini, prema kojem su područjem primjene ove Direktive obuhvaćena sva srednja i velika poduzeća, kako su definirana Preporukom Komisije 2003/361/EZ¹⁵, koja posluju u sektorima ili pružaju vrste usluga na koje se odnosi ova Direktiva. Od država članica ne bi se trebalo zahtijevati sastavljanje popisa subjekata koji ispunjavaju taj općenito primjenjiv kriterij veličine.

Izmjena

(8) ***Odgovornost država članica u*** skladu s Direktivom (EU) 2016/1148, ***po kojoj*** su države članice bile odgovorne za utvrđivanje subjekata koji ispunjavaju kriterije na temelju kojih ih se smatralo operatorima ključnih usluga („postupak utvrđivanja”) ***dovela je do velikih razlika*** među državama članicama u tom pogledu. ***Ne dovodeći u pitanje posebne iznimke predviđene ovom Direktivom***, trebalo bi uspostaviti jedinstveni kriterij za određivanje subjekata obuhvaćenih područjem primjene ove Direktive ***kako bi se uklonile te razlike i osigurala pravna sigurnost u pogledu zahtjeva za upravljanje rizicima i obveza izvješćivanja za sve relevantne subjekte***. Taj bi se kriterij trebao sastojati od primjene pravila o veličini, prema kojem su područjem primjene ove Direktive obuhvaćena sva srednja i velika poduzeća, kako su definirana Preporukom Komisije 2003/361/EZ¹⁵, koja posluju u sektorima ili pružaju vrste usluga na koje se odnosi ova Direktiva. Od država članica ne bi se trebalo zahtijevati sastavljanje popisa subjekata koji ispunjavaju taj općenito primjenjiv kriterij veličine.

¹⁵ Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

¹⁵ Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

Amandman 7

Prijedlog direktive Uvodna izjava 8.a (nova)

Tekst koji je predložila Komisija

Izmjena

(8 a) Uzimajući u obzir razlike u nacionalnim okvirima javne uprave, države članice zadržavaju svoje kapacitete za donošenje odluka u vezi s imenovanjem subjekata u okviru područja primjene ove Direktive.

Amandman 8

Prijedlog direktive Uvodna izjava 9.

Tekst koji je predložila Komisija

Izmjena

(9) **Međutim**, ovom Direktivom trebali bi biti obuhvaćeni i mali subjekti ili mikrosubjekti koji ispunjavaju određene kriterije koji upućuju na ključnu ulogu za gospodarstva ili društva država članica ili za određene sektore ili vrste usluga. Države članice trebale bi biti odgovorne za sastavljanje popisa takvih subjekata i dostaviti ga Komisiji.

(9) Ovom Direktivom trebali bi biti obuhvaćeni i mali subjekti ili mikrosubjekti koji ispunjavaju određene kriterije koji upućuju na ključnu ulogu za gospodarstva ili društva država članica ili za određene sektore ili vrste usluga *na temelju procjene rizika, uključujući subjekte koji su definirani kao kritični subjekti ili subjekti istovjetne kritičnim subjektima u skladu s Direktivom (EU) XXX/XXX Europskog parlamenta i Vijeća^{1a}.* Države članice trebale bi biti odgovorne za sastavljanje popisa takvih subjekata i dostaviti ga Komisiji.

^{1a} Direktiva (EU) [XXX/XXX] Europskog parlamenta i Vijeća od XXX o otpornosti kritičnih subjekata (SL...).

Amandman 9

Prijedlog direktive Uvodna izjava 10.

Tekst koji je predložila Komisija

(10) Komisija u suradnji sa skupinom za suradnju **može** izdati smjernice o provedbi kriterija koji se primjenjuju na **mikropoduzeća i mala poduzeća**.

Izmjena

(10) Komisija **bi** u suradnji sa skupinom za suradnju **trebala** izdati smjernice o provedbi kriterija koji se primjenjuju na **mikrosubjekte i male subjekte**.

Amandman 10

Prijedlog direktive Uvodna izjava 12.

Tekst koji je predložila Komisija

(12) Sektorsko zakonodavstvo i instrumenti mogu pridonijeti osiguravanju visoke razine kibersigurnosti, uzimajući pritom potpuno u obzir posebnosti i složenost tih sektora. Ako se sektorskim pravnim aktom Unije od ključnih ili važnih subjekata zahtjeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavlješćivanje o incidentima ili ozbiljnim kiberprijetnjama koje je po učinku najmanje istovjetno obvezama utvrđenima u ovoj Direktivi, trebale bi se primjenjivati te sektorske odredbe, među ostalim o nadzoru i provedbi. Komisija **može** izdati smjernice o tome kako se primjenjuje lex specialis. Ovom se Direktivom ne sprečava donošenje dodatnih sektorskih akata Unije koji se odnose na mjere upravljanja kibersigurnosnim rizicima i obavlješćivanje o incidentima. Ovom se Direktivom ne dovode u pitanje postojeće provedbene ovlasti dodijeljene Komisiji u brojnim sektorima, uključujući promet i energetiku.

Izmjena

(12) Sektorsko zakonodavstvo i instrumenti mogu pridonijeti osiguravanju visoke razine kibersigurnosti, uzimajući pritom potpuno u obzir posebnosti i složenost tih sektora. Ako se sektorskim pravnim aktom Unije od ključnih ili važnih subjekata zahtjeva donošenje mjera upravljanja kibersigurnosnim rizicima ili obavlješćivanje o incidentima ili ozbiljnim kiberprijetnjama koje je po učinku najmanje istovjetno obvezama utvrđenima u ovoj Direktivi, trebale bi se primjenjivati te sektorske odredbe, među ostalim o nadzoru i provedbi. Komisija **bi trebala** izdati smjernice o tome kako se primjenjuje *lex specialis*. Ovom se Direktivom ne sprečava donošenje dodatnih sektorskih akata Unije koji se odnose na mjere upravljanja kibersigurnosnim rizicima i obavlješćivanje o incidentima. Ovom se Direktivom ne dovode u pitanje postojeće provedbene ovlasti dodijeljene Komisiji u brojnim sektorima, uključujući promet i energetiku.

Amandman 11

Prijedlog direktive Uvodna izjava 14.

Tekst koji je predložila Komisija

(14) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati usklađen pristup između Direktive (EU) XXX/XXX Europskog parlamenta i Vijeća¹⁷ i ove Direktive. Kako bi se to postiglo, države članice trebale bi osigurati da se kritični i ekvivalentni subjekti iz Direktive (EU) XXX/XXX smatraju ključnim subjektima na temelju ove Direktive. Države članice trebale bi osigurati i da se njihovim strategijama za kibersigurnost osigurava okvir politike za bolju koordinaciju između **nadležnog** tijela na temelju ove Direktive i nadležnog tijela na temelju Direktive (EU) XXX/XXX u kontekstu razmjene informacija o **incidentima** i kiberprijetnjama te izvršavanja nadzornih zadaća. Tijela na temelju obiju direktiva trebala bi surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, kiberprijetnji, kibersigurnosnih rizika, incidenata koji utječu na kritične subjekte te kibersigurnosnih mjera koje **ti subjekti** poduzimaju. Na zahtjev nadležnih tijela iz Direktive (EU) XXX/XXX, nadležnim tijelima iz ove Direktive trebalo bi omogućiti **izvršavanje nadzornih i provedbenih ovlasti nad ključnim subjektom** koji je utvrđen kao kritičan. Oba tijela trebala bi surađivati i razmjenjivati informacije u tu svrhu.

Izmjena

(14) S obzirom na međupovezanost kibersigurnosti i fizičke sigurnosti subjekata, trebalo bi osigurati usklađen pristup između Direktive (EU) XXX/XXX Europskog parlamenta i Vijeća¹⁷ i ove Direktive, **gdje god je to moguće i primjereno**. Kako bi se to postiglo, države članice trebale bi osigurati da se kritični i ekvivalentni subjekti iz Direktive (EU) XXX/XXX smatraju ključnim subjektima na temelju ove Direktive. Države članice trebale bi osigurati i da se njihovim strategijama za kibersigurnost osigurava okvir politike za bolju koordinaciju između **nadležnih** tijela **unutar država članica i među njima** na temelju ove Direktive i nadležnog tijela na temelju Direktive (EU) XXX/XXX u kontekstu razmjene informacija o **kiberincidentima** i kiberprijetnjama te izvršavanja nadzornih zadaća. Tijela na temelju obiju direktiva **u državama članicama i među njima** trebala bi surađivati i razmjenjivati informacije, posebno u pogledu utvrđivanja kritičnih subjekata, kiberprijetnji, kibersigurnosnih rizika, incidenata koji utječu na kritične subjekte te kibersigurnosnih mjera koje poduzimaju **nadležna tijela u skladu s ovom Direktivom i koje su relevantne za kritične subjekte**. Na zahtjev nadležnih tijela iz Direktive (EU) XXX/XXX, nadležnim tijelima iz ove Direktive trebalo bi omogućiti **procjenu kibersigurnosti ključnog subjekta** koji je utvrđen kao kritičan. Oba tijela trebala bi surađivati i razmjenjivati informacije u tu svrhu **u stvarnom vremenu**.

¹⁷ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

¹⁷ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

Amandman 12

Prijedlog direkitive Uvodna izjava 18.

Tekst koji je predložila Komisija

(18) Usluge koje nude pružatelji usluga podatkovnog centra ne mogu se uvijek pružati u obliku usluge računalstva u oblaku. Stoga podatkovni centri ne mogu uvijek biti dio infrastrukture računalstva u oblaku. Kako bi se upravljalo svim rizicima za **sigurnost mrežnih i informacijskih sustava**, ovom bi Direktivom trebalo obuhvatiti i pružatelje usluga podatkovnog centra koje nisu usluge računalstva u oblaku. Za potrebe ove Direktive, pojam „usluga podatkovnog centra“ trebao bi obuhvaćati pružanje usluge koja uključuje strukture ili skupine struktura namijenjenih centraliziranim smještaju, međupovezivanju i radu opreme informacijske tehnologije i mreže za usluge pohrane, obrade i prijenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu okoliša. Pojam „usluga podatkovnog centra“ ne primjenjuje se na interne korporativne podatkovne centre kojima predmetni subjekt u čijem su vlasništvu upravlja za vlastite potrebe.

Izmjena

(18) Usluge koje nude pružatelji usluga podatkovnog centra ne mogu se uvijek pružati u obliku usluge računalstva u oblaku. Stoga podatkovni centri ne mogu uvijek biti dio infrastrukture računalstva u oblaku. Kako bi se upravljalo svim rizicima za **kibersigurnost**, ovom bi Direktivom trebalo obuhvatiti i pružatelje usluga podatkovnog centra koje nisu usluge računalstva u oblaku. Za potrebe ove Direktive, pojam „usluga podatkovnog centra“ trebao bi obuhvaćati pružanje usluge koja uključuje strukture ili skupine struktura namijenjenih centraliziranim smještaju, međupovezivanju i radu opreme informacijske tehnologije i mreže za usluge pohrane, obrade i prijenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu okoliša. Pojam „usluga podatkovnog centra“ ne primjenjuje se na interne korporativne podatkovne centre kojima predmetni subjekt u čijem su vlasništvu upravlja za vlastite potrebe.

Amandman 13

Prijedlog direkitive Uvodna izjava 20.

Tekst koji je predložila Komisija

(20) Te rastuće međuovisnosti rezultat su sve veće prekogranične i međuovisne mreže pružanja usluga koja upotrebljava ključnu infrastrukturu diljem Unije u sektorima energetike, prometa, digitalne infrastrukture, vode za piće i otpadne vode, zdravlja, određenih aspekata javne uprave, kao i u svemirskom sektoru u pogledu

Izmjena

(20) Te rastuće međuovisnosti rezultat su sve veće prekogranične i međuovisne mreže pružanja usluga koja upotrebljava ključnu infrastrukturu diljem Unije u sektorima energetike, prometa, digitalne infrastrukture, vode za piće i otpadne vode, **proizvodnje, prerade i distribucije hrane**, zdravlja, određenih aspekata javne uprave,

pružanja određenih usluga koje ovise o zemaljskoj infrastrukturi koja je u vlasništvu i kojom upravljaju države članice ili privatne strane te stoga ne obuhvaća infrastrukturu koja je u vlasništvu Unije, kojom Unija upravlja ili kojom se upravlja u ime Unije kao dijelom njezinih svemirskih programa. Te međuovisnosti znače da svaki poremećaj, čak i onaj koji je prvotno ograničen na jedan subjekt ili jedan sektor, može imati kaskadne učinke u širem smislu, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na pružanje usluga na cijelom unutarnjem tržištu. **Pandemija** bolesti COVID-19 *pokazala je* ranjivost naših sve više međuovisnih društava suočenih s rizicima male vjerovatnosti.

kao i u svemirskom sektoru u pogledu pružanja određenih usluga koje ovise o zemaljskoj infrastrukturi koja je u vlasništvu i kojom upravljaju države članice ili privatne strane te stoga ne obuhvaća infrastrukturu koja je u vlasništvu Unije, kojom Unija upravlja ili kojom se upravlja u ime Unije kao dijelom njezinih svemirskih programa. Te međuovisnosti znače da svaki poremećaj, čak i onaj koji je prvotno ograničen na jedan subjekt ili jedan sektor, može imati kaskadne učinke u širem smislu, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na pružanje usluga na cijelom unutarnjem tržištu. **Intenzivniji napadi na informacijske sustave tijekom pandemije** bolesti COVID-19 *pokazali su* ranjivost naših sve više međuovisnih društava suočenih s rizicima male vjerovatnosti. **Stoga su potrebna daljnja ulaganja u kibersigurnost.**

Amandman 14

Prijedlog direktive Uvodna izjava 20.a (nova)

Tekst koji je predložila Komisija

Izmjena

(20 a) Ključno je podići razinu osviještenosti o kiberprostoru i kiberotpornosti u svim ključnim i važnim subjektima, uključujući tijela javne uprave.

Amandman 15

Prijedlog direktive Uvodna izjava 21.

Tekst koji je predložila Komisija

Izmjena

(21) S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite

(21) S obzirom na razlike u nacionalnim upravljačkim strukturama i radi zaštite

postojećih sektorskih rješenja ili nadzornih i regulatornih tijela Unije, države članice trebale bi moći imenovati više od jednog nadležnog nacionalnog tijela odgovornog za izvršavanje zadaća povezanih sa sigurnošću mrežnih i informacijskih sustava ključnih i važnih subjekata obuhvaćenih ovom Direktivom. Države članice trebale bi moći tu ulogu dodijeliti postojećem tijelu.

postojećih sektorskih rješenja ili nadzornih i regulatornih tijela Unije, države članice trebale bi moći imenovati više od jednog nadležnog nacionalnog tijela odgovornog za izvršavanje zadaća povezanih sa sigurnošću mrežnih i informacijskih sustava ključnih i važnih subjekata obuhvaćenih ovom Direktivom. Države članice trebale bi moći tu ulogu dodijeliti postojećem tijelu *i osigurati da ima odgovarajuća sredstva za djelotvorno i učinkovito izvršavanje svojih zadaća.*

Amandman 16

Prijedlog direktive Uvodna izjava 22.

Tekst koji je predložila Komisija

(22) Da bi se olakšala prekogranična suradnja i komunikacija među tijelima i da bi se omogućila djelotvorna provedba ove Direktive, nužno je da svaka država članica imenuje jedinstvenu nacionalnu kontaktnu točku odgovornu za koordinaciju pitanja ***sigurnosti mrežnih i informacijskih sustava*** te za prekograničnu suradnju na razini Unije.

Izmjena

(22) Da bi se olakšala prekogranična suradnja i komunikacija među tijelima i da bi se omogućila djelotvorna provedba ove Direktive, nužno je da svaka država članica imenuje jedinstvenu nacionalnu kontaktnu točku odgovornu za koordinaciju pitanja ***kibersigurnosti*** te za prekograničnu suradnju na razini Unije.

Amandman 17

Prijedlog direktive Uvodna izjava 23.

Tekst koji je predložila Komisija

(23) Nadležna tijela ili CSIRT-ovi trebali bi od subjekata primati obavijesti o incidentima na djelotvoran i učinkovit način. Zadaća jedinstvenih kontaktnih točaka trebala bi biti proslijđivanje obavijesti o incidentima jedinstvenim kontaktnim točkama drugih pogodjenih država članica. Kako bi se osigurala jedinstvena ulazna točka u svakoj državi članici, jedinstvene kontaktne točke na

Izmjena

(23) Nadležna tijela ili CSIRT-ovi trebali bi od subjekata primati obavijesti o incidentima na djelotvoran i učinkovit način. Zadaća jedinstvenih kontaktnih točaka trebala bi biti proslijđivanje obavijesti o incidentima ***u stvarnom vremenu*** jedinstvenim kontaktnim točkama ***svih drugih*** pogodjenih država članica. Kako bi se osigurala jedinstvena ulazna točka u svakoj državi članici, jedinstvene

razini tijela država članica trebale bi primati relevantne informacije o incidentima koji se odnose na subjekte finansijskog sektora od nadležnih tijela iz Uredbe XXXX/XXXX koje bi, prema potrebi, trebale moći proslijediti relevantnim nacionalnim nadležnim tijelima ili CSIRT-ovima iz ove Direktive.

kontaktne točke na razini tijela država članica trebale bi primati relevantne informacije o incidentima koji se odnose na subjekte finansijskog sektora od nadležnih tijela iz Uredbe XXXX/XXXX koje bi, prema potrebi, trebale moći proslijediti relevantnim nacionalnim nadležnim tijelima ili CSIRT-ovima iz ove Direktive.

Amandman 18

Prijedlog direktive Uvodna izjava 25.

Tekst koji je predložila Komisija

(25) Kad je riječ o osobnim podacima, CSIRT-ovi bi, u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća¹⁹ o osobnim podacima, u ime subjekta iz ove Direktive i na njegov zahtjev, trebali moći osigurati **proaktivno** pregledavanje mrežnih i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga. Države članice trebale bi nastojati osigurati jednaku razinu tehničkih sposobnosti za sve sektorske CSIRT-ove. Države članice mogu zatražiti pomoć Agencije Europske unije za kibersigurnost (ENISA) u razvoju nacionalnih CSIRT-ova.

Izmjena

(25) Kad je riječ o osobnim podacima, CSIRT-ovi bi, u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća¹⁹ i Direktivom 2002/58/EZ, u ime subjekta iz ove Direktive i na njegov zahtjev, trebali moći osigurati **sigurnosno** pregledavanje informacijskih sustava i **mrežni domet** koji se upotrebljavaju za pružanje njihovih usluga **kako bi se prepoznale, ublažile ili spriječile specifične prijetnje**. Države članice trebale bi nastojati osigurati jednaku razinu tehničkih sposobnosti za sve sektorske CSIRT-ove. Države članice mogu zatražiti pomoć Agencije Europske unije za kibersigurnost (ENISA) u razvoju nacionalnih CSIRT-ova. **Nadalje, rizici povezani s kibersigurnošću nikada se ne bi smjeli upotrebljavati kao izgovor za kršenje temeljnih prava.**

¹⁹ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

¹⁹ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

Amandman 19

Prijedlog direktive Uvodna izjava 27.

Tekst koji je predložila Komisija

(27) U skladu s Prilogom Preporuci Komisije (EU) 2017/1548 o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera („plan“)²⁰, incident velikih razmjera trebao bi značiti incident sa znatnim utjecajem na najmanje dvije države članice ili incident čiji učinci premašuju sposobnost države članice da na njega odgovori. Ovisno o svojem uzroku i utjecaju, incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor u cijeloj Uniji.

Izmjena

(27) U skladu s Prilogom Preporuci Komisije (EU) 2017/1548 o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera („plan“)²⁰, incident velikih razmjera trebao bi značiti incident sa znatnim utjecajem na najmanje dvije države članice ili incident čiji učinci premašuju sposobnost države članice da na njega odgovori. Ovisno o svojem uzroku i utjecaju, incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta *ili predstavljaju ozbiljne rizike za javnu sigurnost u nekoliko država članica ili u Uniji kao cjelini*. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor u cijeloj Uniji.

Države članice trebale bi zajednički pratiti način provedbe pravila EU-a, međusobno si pomagati u slučaju bilo kakvih prekograničnih problema, uspostaviti strukturiraniji dijalog s privatnim sektorom i surađivati u pogledu sigurnosnih rizika i prijetnji povezanih s novim tehnologijama, kao što je bio slučaj s tehnologijom 5G.

²⁰ Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

²⁰ Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

Amandman 20

Prijedlog direktive Uvodna izjava 33.

Tekst koji je predložila Komisija

(33) Pri izradi smjernica skupina za suradnju trebala bi biti dosljedna u: mapiranju nacionalnih rješenja i iskustava, procjenjivanju učinka rezultata skupine za suradnju na nacionalne pristupe, raspravljanju o izazovima u provedbi i izradi posebnih preporuka koje će se nastojati ispuniti boljom provedbom postojećih pravila.

Izmjena

(33) Pri izradi smjernica skupina za suradnju trebala bi biti dosljedna u: mapiranju nacionalnih *i sektorskih* rješenja i iskustava, procjenjivanju učinka rezultata skupine za suradnju na nacionalne *i sektorske* pristupe, raspravljanju o izazovima u provedbi i izradi posebnih preporuka koje će se nastojati ispuniti boljom provedbom postojećih pravila.

Amandman 21

Prijedlog direktive Uvodna izjava 34.

Tekst koji je predložila Komisija

(34) Skupina za suradnju trebala bi ostati fleksibilan forum i trebala bi moći odgovoriti na nove i promjenjive političke prioritete i izazove, uzimajući pritom u obzir raspoloživost resursa. Trebala bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima iz cijele Unije na kojima bi se raspravljalo o aktivnostima skupine i prikupljale informacije o novim političkim izazovima. Kako bi se poboljšala suradnja na razini Unije, skupina bi trebala *razmotriti mogućnost pozivanja* tijela i *agencija* Unije *uključenih* u politiku kibersigurnosti, *kao što su Europski centar za kiberkriminalitet (EC3), Agencija* Europske unije za sigurnost zračnog prometa (EASA) i *Agencija* Europske unije za svemirski program (EUSPA), da sudjeluju u njezinu radu.

Izmjena

(34) Skupina za suradnju trebala bi ostati fleksibilan forum i trebala bi moći odgovoriti na nove i promjenjive političke prioritete i izazove, uzimajući pritom u obzir raspoloživost resursa. Trebala bi organizirati redovite zajedničke sastanke s relevantnim privatnim dionicima iz cijele Unije na kojima bi se raspravljalo o aktivnostima skupine i prikupljale informacije o novim političkim izazovima. Kako bi se poboljšala suradnja na razini Unije, skupina bi trebala *pozvati nadležna tijela i agencije* Unije *uključene* u politiku kibersigurnosti, *posebno Europol, Agenciju* Europske unije za sigurnost zračnog prometa (EASA) i *Agenciju* Europske unije za svemirski program (EUSPA), da sudjeluju u njezinu radu.

Amandman 22

Prijedlog direktive Uvodna izjava 36.

Tekst koji je predložila Komisija

(36) Unija bi, prema potrebi, trebala sklapati međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama, u skladu s člankom 218. UFEU-a, kojima im se dopušta i organizira sudjelovanje u nekim aktivnostima skupine za suradnju i mreže CSIRT-ova. *Takovim bi se sporazumima trebala osigurati odgovarajuća zaštita podataka.*

Izmjena

(36) Unija bi, prema potrebi, trebala sklapati međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama, u skladu s člankom 218. UFEU-a, kojima im se dopušta i organizira sudjelovanje u nekim aktivnostima skupine za suradnju i mreže CSIRT-ova. *U mjeri u kojoj se osobni podaci prenose trećoj zemlji ili medunarodnoj organizaciji trebalo bi primjenjivati poglavlje V. Uredbe (EU) 2016/679.*

Amandman 23

Prijedlog direktive Uvodna izjava 37.

Tekst koji je predložila Komisija

(37) Države članice trebale bi doprinijeti uspostavi okvira EU-a za odgovor na kiberkrize utvrđenog u Preporuci (EU) 2017/1584 putem postojećih mreža suradnje, posebno Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe), mreže CSIRT-ova i skupine za suradnju. EU-CyCLONe i mreža CSIRT-ova trebali bi surađivati na temelju postupovnih aranžmana kojima se utvrđuju načini te suradnje. U poslovniku EU-CyCLONe-a trebalo bi dodatno utvrditi načine funkcioniranja mreže, uključujući, među ostalim, uloge, oblike suradnje, interakcije s drugim relevantnim akterima i predloške za razmjenu informacija, kao i komunikacijska sredstva. Za upravljanje krizama na razini Unije relevantne strane trebale bi se oslanjati na aranžmane za integrirani politički odgovor na krizu (IPCR). Komisija bi u tu svrhu trebala primjenjivati međusektorski postupak

Izmjena

(37) Države članice trebale bi doprinijeti uspostavi okvira EU-a za odgovor na kiberkrize utvrđenog u Preporuci (EU) 2017/1584 putem postojećih mreža suradnje, posebno Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe), mreže CSIRT-ova i skupine za suradnju. EU-CyCLONe i mreža CSIRT-ova trebali bi surađivati na temelju postupovnih aranžmana kojima se utvrđuju načini te suradnje. U poslovniku EU-CyCLONe-a trebalo bi dodatno utvrditi načine funkcioniranja mreže, uključujući, među ostalim, uloge, oblike suradnje, interakcije s drugim relevantnim akterima i predloške za razmjenu informacija, kao i komunikacijska sredstva. Za upravljanje krizama na razini Unije relevantne strane trebale bi se oslanjati na aranžmane za integrirani politički odgovor na krizu (IPCR). Komisija bi u tu svrhu trebala primjenjivati međusektorski postupak

koordiniranja krize na visokoj razini ARGUS. Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), trebalo bi aktivirati mehanizam za odgovor na krize (CRM) Europske službe za vanjsko djelovanje (ESVD).

koordiniranja krize na visokoj razini ARGUS. *Ako se kriza odnosi na dvije ili više država članica i ako se sumnja da je kriminalne prirode*, trebalo bi *razmotriti aktivaciju Protokola EU-a za odgovor tijela kaznenog progona na krizne situacije*. Ako kriza ima znatan utjecaj na vanjsku ili zajedničku sigurnosnu i obrambenu politiku (ZSOP), trebalo bi aktivirati mehanizam za odgovor na krize (CRM) Europske službe za vanjsko djelovanje (ESVD).

Amandman 24

Prijedlog direktive Uvodna izjava 45.

Tekst koji je predložila Komisija

(45) Subjekti bi trebali raditi i na suzbijanju kibersigurnosnih rizika koji proizlaze iz njihove interakcije i odnosa s drugim dionicima unutar šireg ekosustava. Konkretno, subjekti bi trebali poduzeti odgovarajuće mjere kako bi osigurali da se njihova suradnja s akademskim i istraživačkim institucijama odvija u skladu s njihovim kibersigurnosnim politikama i da slijedi dobre prakse u pogledu sigurnog pristupa informacijama i širenja informacija općenito, a posebno u pogledu zaštite intelektualnog vlasništva. Slično tome, s obzirom na važnost i vrijednost podataka za aktivnosti subjekata, pri oslanjanju na usluge transformacije i analize podataka koje pružaju treće strane subjekti bi trebali poduzeti sve odgovarajuće kibersigurnosne mjere.

Izmjena

(45) Subjekti bi trebali raditi i na suzbijanju kibersigurnosnih rizika koji proizlaze iz njihove interakcije i odnosa s drugim dionicima unutar šireg ekosustava. Konkretno, subjekti bi trebali poduzeti odgovarajuće mjere kako bi osigurali da se njihova suradnja s akademskim i istraživačkim institucijama odvija u skladu s njihovim kibersigurnosnim politikama i da slijedi dobre prakse u pogledu sigurnog pristupa informacijama i širenja informacija općenito, a posebno u pogledu zaštite intelektualnog vlasništva. Slično tome, s obzirom na važnost i vrijednost podataka za aktivnosti subjekata, pri oslanjanju na usluge transformacije i analize podataka koje pružaju treće strane subjekti bi trebali poduzeti sve odgovarajuće kibersigurnosne mjere *i prijaviti svaki potencijalni kibernapad koji utvrde*.

Amandman 25

Prijedlog direktive Uvodna izjava 46.a (nova)

Tekst koji je predložila Komisija

Izmjena

(46 a) Posebna bi se pozornost trebala posvetiti slučajevima kad IKT usluge, sustavi ili proizvodi podliježu posebnim zahtjevima u zemlji podrijetla koji bi mogli dovesti do prepreka za usklađenost sa zakonodavstvom EU-a o privatnosti i zaštiti podataka. U okviru takvih procjena rizika trebalo bi se, prema potrebi, posavjetovati s Europskim odborom za zaštitu podataka. Besplatan softver otvorenog koda i hardver otvorenog koda mogli bi donijeti velike koristi za kibersigurnost, posebno u pogledu transparentnosti i provjerljivosti značajki. Budući da bi to moglo pomoći u uklanjanju i ublažavanju specifičnih rizika u lancu opskrbe, trebalo bi im dati prednost ako je to izvedivo u skladu s Mišljenjem br. 5/2021 Europskog nadzornika za zaštitu podataka^{1a}.

^{1a} Mišljenje 5/2021 Europskog nadzornika za zaštitu podataka o strategiji za kibersigurnost i Direktivi NIS 2.0, 11. ožujka 2021.

Amandman 26

Prijedlog direkture Uvodna izjava 47.

Tekst koji je predložila Komisija

(47) U procjenama rizika u lancu opskrbe, s obzirom na značajke predmetnog sektora, trebalo bi uzeti u obzir tehničke i, prema potrebi, netehničke čimbenike, **uključujući** one definirane u Preporuci (EU) 2019/534, u usklađenoj procjeni rizika sigurnosti 5G mreža na razini EU-a i u paketu instrumenata EU-a za kibersigurnost 5G tehnologije oko kojih se suglasila skupina za suradnju. Pri utvrđivanju lanaca opskrbe koji bi trebali

Izmjena

(47) U procjenama rizika u lancu opskrbe, s obzirom na značajke predmetnog sektora, trebalo bi uzeti u obzir tehničke i, prema potrebi, netehničke čimbenike **koje bi skupina za suradnju trebala dodatno precizirati i koji uključuju** one definirane u Preporuci (EU) 2019/534, u usklađenoj procjeni rizika sigurnosti 5G mreža na razini EU-a i u paketu instrumenata EU-a za kibersigurnost 5G tehnologije oko kojih se suglasila skupina

biti podložni koordiniranoj procjeni rizika, u obzir bi trebalo uzeti sljedeće kriterije: *i.* i. mjera u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, sustavima ili proizvodima i oslanjaju na njih; ii. važnost specifičnih ključnih IKT usluga, sustava ili proizvoda u obavljanju ključnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; iii. dostupnost alternativnih IKT usluga, sustava ili proizvoda; iv. otpornost cjelokupnog lanca opskrbe IKT uslugama, sustavima ili proizvodima na ometajuće događaje i v. potencijalna buduća važnost novih IKT usluga, sustava ili proizvoda za aktivnosti subjekata.

za suradnju. Pri utvrđivanju lanaca opskrbe koji bi trebali biti podložni koordiniranoj procjeni rizika, u obzir bi trebalo uzeti sljedeće kriterije: i. mjera u kojoj se ključni i važni subjekti koriste određenim ključnim IKT uslugama, sustavima ili proizvodima i oslanjaju na njih; ii. važnost specifičnih ključnih IKT usluga, sustava ili proizvoda u obavljanju ključnih ili osjetljivih funkcija, uključujući obradu osobnih podataka; iii. dostupnost alternativnih IKT usluga, sustava ili proizvoda; iv. otpornost cjelokupnog lanca opskrbe IKT uslugama, sustavima ili proizvodima na ometajuće događaje i v. potencijalna buduća važnost novih IKT usluga, sustava ili proizvoda za aktivnosti subjekata.

Amandman 27

Prijedlog direktive Uvodna izjava 48.a (nova)

Tekst koji je predložila Komisija

Izmjena

(48.a) Mala i srednja poduzeća (MSP-ovi) često nisu dovoljno velika i nemaju dovoljno sredstava da zadovolje širok i sve veći spektar kibersigurnosnih potreba u međupovezanom svijetu, u kojem sve više osoba radi na daljinu. Države članice stoga bi u svoje nacionalne strategije za kibersigurnost trebale uključiti smjernice i potporu za MSP-ove.

Amandman 28

Prijedlog direktive Uvodna izjava 50.

Tekst koji je predložila Komisija

Izmjena

(50) S obzirom na sve veću važnost brojevno neovisnih interpersonalnih komunikacijskih usluga, potrebno je osigurati da se i na takve usluge primjenjuju odgovarajući sigurnosni zahtjevi u skladu s njihovim posebnostima

(50) S obzirom na sve veću važnost brojevno neovisnih interpersonalnih komunikacijskih usluga, potrebno je osigurati da se i na takve usluge primjenjuju odgovarajući sigurnosni zahtjevi u skladu s njihovim posebnostima

i gospodarskom važnošću. Stoga bi pružatelji takvih usluga trebali osigurati i odgovarajuću razinu ***sigurnosti mrežnih i informacijskih sustava*** obzirom na rizik kojem su izloženi. S obzirom na to da pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga obično nemaju stvarnu kontrolu nad prijenosom signala mrežama, stupanj rizika za takve usluge može se u nekim aspektima smatrati nižim od rizika za tradicionalne elektroničke komunikacijske usluge. Isto bi trebalo primijeniti na interpersonalne komunikacijske usluge koje se koriste brojevima, a koje nemaju stvarnu kontrolu nad prijenosom signala mrežama.

Amandman 29

Prijedlog direkutive Uvodna izjava 52.

Tekst koji je predložila Komisija

(52) Prema potrebi, subjekti bi trebali obavijestiti svoje primatelje usluga o posebnim i ozbiljnim prijetnjama te o mjerama koje mogu poduzeti kako bi ublažili nastali rizik. Zahtjev obavljanja primatelja usluga o takvim prijetnjama ne bi smio podrazumijevati oslobođanje pružatelja od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mјere kako bi se spriječile ili uklonile sve kiberprijetnje i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o sigurnosnim prijetnjama trebalo bi biti besplatno za primatelje usluga.

Amandman 30

Prijedlog direkutive Uvodna izjava 53.

Tekst koji je predložila Komisija

(53) Pružatelji javnih elektroničkih

i gospodarskom važnošću. Stoga bi pružatelji takvih usluga trebali osigurati i odgovarajuću razinu ***kibersigurnosti s*** obzirom na rizik kojem su izloženi. S obzirom na to da pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga obično nemaju stvarnu kontrolu nad prijenosom signala mrežama, stupanj rizika za takve usluge može se u nekim aspektima smatrati nižim od rizika za tradicionalne elektroničke komunikacijske usluge. Isto bi trebalo primijeniti na interpersonalne komunikacijske usluge koje se koriste brojevima, a koje nemaju stvarnu kontrolu nad prijenosom signala mrežama.

Izmjena

(52) Prema potrebi, subjekti bi trebali ***imati mogućnost*** obavijestiti svoje primatelje usluga o posebnim i ozbiljnim prijetnjama te o mjerama koje mogu poduzeti kako bi ublažili nastali rizik. Zahtjev obavljanja primatelja usluga o takvim prijetnjama ne bi smio podrazumijevati oslobođanje pružatelja od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mјere kako bi se spriječile ili uklonile sve kiberprijetnje i ponovno uspostavila normalna sigurnosna razina usluge. Pružanje takvih informacija o sigurnosnim prijetnjama trebalo bi biti besplatno za primatelje usluga.

Izmjena

(53) Pružatelji javnih elektroničkih

komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga trebali bi obavijestiti primatelje usluga o posebnim i ozbiljnim kiberprijetnjama te o mjerama koje mogu poduzeti kako bi očuvali sigurnost svojih komunikacija, na primjer upotrebom posebnih vrsta softvera ili tehnologija šifriranja.

komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga trebali bi *primjenjivati načela integrirane i zadane sigurnost i* obavijestiti primatelje usluga o posebnim i ozbiljnim kiberprijetnjama te o mjerama koje mogu poduzeti kako bi očuvali sigurnost svojih *uredaja i* komunikacija, na primjer upotrebom posebnih vrsta softvera ili tehnologija šifriranja. *Kako bi se povećala sigurnost hardvera i softvera, pružatelje bi trebalo poticati da se koriste otvorenim kodom i otvorenim hardverom.*

Amandman 31

Prijedlog direktive Uvodna izjava 54.

Tekst koji je predložila Komisija

(54) Kako bi se zaštitila sigurnost elektroničkih komunikacijskih mreža i usluga, trebalo bi promicati upotrebu šifriranja, posebice šifriranja s kraja na kraj, koja bi, prema potrebi, trebala biti obvezna za pružatelje takvih usluga i mreža u skladu s načelima zadane i integrirane sigurnosti i privatnosti u smislu članka 18. Upotrebu šifriranja s kraja na kraj trebalo bi uskladiti s *ovlastima* država članica da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste *istragu*, otkrivanje i progona kaznenih djela u skladu s pravom Unije. Rješenjima za zakonit pristup informacijama u komunikacijama šifriranima s kraja na kraj trebala bi se očuvati učinkovitost šifriranja u zaštiti privatnosti i sigurnosti komunikacija *te* bi se *istodobno trebao osigurati učinkovit odgovor na kriminal*.

Izmjena

(54) Kako bi se zaštitila sigurnost elektroničkih komunikacijskih mreža i usluga, *kao i temeljna prava na zaštitu podataka i privatnost* trebalo bi promicati upotrebu šifriranja, posebice šifriranja s kraja na kraj, koja bi, prema potrebi, trebala biti obvezna za pružatelje takvih usluga i mreža u skladu s načelima zadane i integrirane sigurnosti i privatnosti u smislu članka 18. Upotrebu šifriranja s kraja na kraj trebalo bi uskladiti s *odgovornošću* država članica da osiguraju zaštitu svojih ključnih sigurnosnih interesa i javne sigurnosti te da dopuste *sprečavanje*, otkrivanje i progona kaznenih djela u skladu s pravom Unije *i nacionalnim pravom*. Rješenjima za zakonit pristup informacijama u komunikacijama šifriranima s kraja na kraj trebala bi se očuvati učinkovitost šifriranja u zaštiti privatnosti i sigurnosti komunikacija. *Ništa u ovoj Uredbi ne bi trebalo promatrati kao pokušaj slabljenja šifriranja s kraja na kraj s pomoću „backdoor“ pristupa ili sličnih rješenja jer se nedostaci u šifriranju mogu iskoristiti u zlonamjerne svrhe. Svaka mjera*

usmjeren na slabljenje šifriranja ili zaobilazeњe arhitekture te tehnologije može prouzročiti znatne rizike za sposobnost učinkovite zaštite koju ona podrazumijeva. Trebalo bi zabraniti svako neovlašteno dešifriranje ili praćenje elektroničkih komunikacija koje ne provode pravna tijela kako bi se osigurala učinkovitost tehnologije i njezina šira uporaba. Važno je da se države članice pozabave problemima s kojima se susreću pravna tijela i istraživači ranjivosti. U nekim državama članicama subjekti i fizičke osobe koji istražuju ranjivosti izloženi su kaznenoj i građanskoj odgovornosti. Stoga se države članice potiče da izdaju smjernice za izuzeće od kaznenog progona i odgovornosti za istraživanja u području informacijske sigurnosti.

Amandman 32

Prijedlog direktive Uvodna izjava 56.

Tekst koji je predložila Komisija

(56) Ključni i važni subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavlješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatna opterećenja i mogu dovesti do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. S obzirom na to i u svrhu pojednostavljenja izvješćivanja o sigurnosnim incidentima, države članice trebale bi uspostaviti jedinstvenu ulaznu točku **za sve obavijesti koje se zahtijevaju** ovom Direktivom i drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. ENISA bi sa skupinom za suradnju trebala izraditi zajedničke predloške za obavlješćivanje s pomoću smjernica kojima bi se pojednostavnile i uskladile izvještajne informacije koje se zahtijevaju pravom

Izmjena

(56) Ključni i važni subjekti često određeni incident, zbog njegovih značajki, moraju prijaviti različitim tijelima u skladu s obvezama obavlješćivanja uključenima u razne pravne instrumente. Takvi slučajevi stvaraju dodatna opterećenja i mogu dovesti do nesigurnosti u pogledu oblika obavijesti i postupanja s njima. S obzirom na to i u svrhu pojednostavljenja izvješćivanja o sigurnosnim incidentima, države članice trebale bi uspostaviti jedinstvenu ulaznu točku **koja se zahtijeva** ovom Direktivom i drugim pravom Unije, kao što su Uredba (EU) 2016/679 i Direktiva 2002/58/EZ. ENISA bi sa skupinom za suradnju **i Europskim odborom za zaštitu podataka** trebala izraditi zajedničke predloške za obavlješćivanje s pomoću smjernica kojima bi se pojednostavnile i uskladile izvještajne

Unije, čime bi se smanjilo opterećenje za poduzeća.

informacije koje se zahtijevaju pravom Unije, čime bi se smanjilo opterećenje za poduzeća.

Amandman 33

Prijedlog direkitive Uvodna izjava 57.

Tekst koji je predložila Komisija

(57) Ako se sumnja da je incident povezan s aktivnostima koje se prema pravu Unije ili nacionalnom pravu smatraju ozbiljnim kriminalnim aktivnostima, države članice trebale bi ključne i važne subjekte poticati da, na temelju primjenjivih pravila kaznenog postupka u skladu s pravom Unije, relevantnim tijelima za izvršavanje zakonodavstva prijave incidente za koje se sumnja da su ozbiljne kriminalne naravi. Prema potrebi i ne dovodeći u pitanje pravila o zaštiti osobnih podataka koja se primjenjuju na Europol, poželjno je da EC3 i ENISA olakšavaju koordinaciju između nadležnih tijela i tijela za izvršavanje zakonodavstva različitih država članica.

Izmjena

(57) Ako se sumnja da je incident povezan s aktivnostima koje se prema pravu Unije ili nacionalnom pravu smatraju ozbiljnim kriminalnim aktivnostima, države članice trebale bi ključne i važne subjekte poticati da, na temelju primjenjivih pravila kaznenog postupka u skladu s pravom Unije, relevantnim tijelima za izvršavanje zakonodavstva prijave incidente za koje se sumnja da su ozbiljne kriminalne naravi. Prema potrebi i ne dovodeći u pitanje pravila o zaštiti osobnih podataka koja se primjenjuju na Europol, poželjno je da **Europski centar za kiberkriminalitet (EC3) u okviru Europol-a** i ENISA olakšavaju koordinaciju između nadležnih tijela i tijela za izvršavanje zakonodavstva različitih država članica.

Amandman 34

Prijedlog direkitive Uvodna izjava 58.

Tekst koji je predložila Komisija

(58) U mnogim slučajevima osobni podaci ugroženi su zbog incidenata. U tom kontekstu nadležna tijela trebala bi surađivati i razmjenjivati informacije o svim relevantnim pitanjima s tijelima za zaštitu podataka i nadzornim tijelima u skladu s Direktivom 2002/58/EZ.

Izmjena

(58) U mnogim slučajevima osobni podaci ugroženi su zbog incidenata. U tom kontekstu nadležna tijela trebala bi surađivati i razmjenjivati informacije o svim relevantnim pitanjima s tijelima za zaštitu podataka i nadzornim tijelima u skladu s **Uredbom (EU) 2016/679 i Direktivom 2002/58/EZ**.

Amandman 35

Prijedlog direktive Uvodna izjava 59.

Tekst koji je predložila Komisija

(59) Vođenje točnih i potpunih baza podataka s nazivima domena i registracijskim podacima (tzv. podaci WHOIS) te omogućivanje zakonitog pristupa takvim podacima ključni su za osiguravanje sigurnosti, stabilnosti i otpornosti DNS-a, što pridonosi visokoj zajedničkoj razini kibersigurnosti u Uniji. Obrada koja uključuje osobne podatke mora biti u skladu s pravom Unije o zaštiti podataka.

Izmjena

(59) Vođenje točnih i potpunih baza podataka s nazivima domena i registracijskim podacima (tzv. podaci WHOIS) te omogućivanje zakonitog pristupa takvim podacima ključni su za osiguravanje sigurnosti, stabilnosti i otpornosti DNS-a, što pridonosi visokoj zajedničkoj razini kibersigurnosti u Uniji. Obrada koja uključuje osobne podatke mora biti u skladu s **primjenjivim** pravom Unije o zaštiti podataka.

Amandman 36

Prijedlog direktive Uvodna izjava 62.

Tekst koji je predložila Komisija

(62) Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi objaviti podatke o registraciji naziva domena **koji nisu obuhvaćeni područjem primjene pravila Unije o zaštiti podataka, kao što su podaci o pravnim osobama**. Registri vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu trebali bi usto zakonitim tražiteljima pristupa omogućiti legalan pristup podacima o registraciji određenih naziva domena koji se odnose na fizičke osobe, u skladu s **pravom Unije o zaštiti podataka**. Države članice trebale bi osigurati da registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena bez nepotrebne odgode odgovaraju na zahtjeve za otkrivanje podataka o registraciji naziva domena **koje**

Izmjena

(62) **Radi ispunjavanja pravnih obveza u odredbama članka 6. stavka 1. točke (c),** Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi objaviti podatke o registraciji naziva **određenih** domena **navedenih u zakonu državu članice kojem podliježe, poput naziva domene i pravne osobe**. Registri vršnih domena i subjekti koji **im** pružaju usluge registracije naziva domena za vršnu domenu trebali bi usto zakonitim tražiteljima pristupa omogućiti legalan pristup podacima o registraciji određenih naziva domena koji se odnose na fizičke osobe, **prije svega nadležnih tijela u okviru ove Direktive ili nadzornih tijela u okviru Uredbe (EU) 2016/679** u skladu s **njihovim ovlastima**. Države članice trebale bi osigurati da registri vršnih domena i subjekti koji im pružaju usluge registracije

upute zakoniti tražitelji pristupa. Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi uspostaviti politike i postupke za objavljivanje i otkrivanje registracijskih podataka, uključujući sporazume o razini usluga za rješavanje zahtjeva za pristup zakonitih tražitelja pristupa. Postupak pristupa može uključivati i upotrebu sučelja, portala ili drugog tehničkog alata kako bi se osigurao učinkovit sustav za podnošenje zahtjeva i pristupanje registracijskim podacima. U cilju promicanja usklađenih praksi na unutarnjem tržištu, Komisija može donijeti smjernice o takvim postupcima ne dovodeći u pitanje nadležnosti Europskog odbora za zaštitu podataka.

naziva domena bez nepotrebne odgode odgovaraju na *zakonite i propisno obrazložene zahtjeve javnih tijela, uključujući nadležna tijela u skladu s ovom Direktivom, nadležna tijela u skladu s pravom Unije ili nacionalnim pravom za sprečavanje, istragu ili progon kaznenih djela ili nadzorna tijela u skladu s Uredbom (EU) 2016/679*, za otkrivanje podataka o registraciji naziva domena. Registri vršnih domena i subjekti koji im pružaju usluge registracije naziva domena trebali bi uspostaviti politike i postupke za objavljivanje i otkrivanje registracijskih podataka, uključujući sporazume o razini usluga za rješavanje zahtjeva za pristup zakonitih tražitelja pristupa. Postupak pristupa može uključivati i upotrebu sučelja, portala ili drugog tehničkog alata kako bi se osigurao učinkovit sustav za podnošenje zahtjeva i pristupanje registracijskim podacima. U cilju promicanja usklađenih praksi na unutarnjem tržištu, Komisija može donijeti smjernice o takvim postupcima ne dovodeći u pitanje nadležnosti Europskog odbora za zaštitu podataka.

²⁵ *U uvodnoj izjavi 14. UREDBE (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA navodi se: „Ovom se Uredbom ne obuhvaća obrada osobnih podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe”.*

Amandman 37

Prijedlog direktive Uvodna izjava 63.

Tekst koji je predložila Komisija

(63) *Svi* ključni i važni subjekti obuhvaćeni ovom Direktivom trebali bi biti

Izmjena

(63) *U svrhu ove Direktive* *svi* ključni i važni subjekti obuhvaćeni ovom

u nadležnosti države članice u kojoj pružaju usluge. Ako subjekt pruža usluge u više država članica, trebao bi biti u zasebnoj i istodobnoj nadležnosti svake od tih država članica. Nadležna tijela tih država članica trebala bi suradivati, međusobno si pomagati i, prema potrebi, provoditi zajedničke nadzorne aktivnosti.

Direktivom trebali bi biti u nadležnosti države članice u kojoj pružaju usluge. Ako subjekt pruža usluge u više država članica, trebao bi biti u zasebnoj i istodobnoj nadležnosti svake od tih država članica. Nadležna tijela tih država članica trebala bi **se dogovoriti oko sastavnih klasifikacija**, suradivati **gdje god je to moguće**, međusobno si pomagati i, prema potrebi, provoditi zajedničke nadzorne aktivnosti **u stvarnom vremenu**.

Amandman 38

Prijedlog direkitive Uvodna izjava 64.

Tekst koji je predložila Komisija

(64) Kako bi se u obzir uzela prekogranična priroda usluga i aktivnosti pružatelja DNS usluga, registara naziva vršnih domena, pružatelja mreža za isporuku sadržaja, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra i pružatelja digitalnih usluga, samo bi jedna država članica trebala imati nadležnost nad tim subjektima. Nadležnost bi se trebala dodijeliti državi članici u kojoj predmetni subjekt ima glavni poslovni nastan u Uniji. Kriterij poslovnog nastana za potrebe ove Direktive podrazumijeva učinkovito obavljanje djelatnosti putem stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo kroz podružnicu bilo društvo kćer s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu. Ispunjene tog kriterija ne bi trebalo ovisiti o tome jesu li mrežni i informacijski sustavi fizički smješteni na određenom mjestu; postojanje i upotreba takvih sustava sami po sebi ne čine takav glavni poslovni nastan i stoga nisu odlučujući kriteriji za određivanje glavnog poslovnog nastana. Glavni poslovni nastan trebao bi biti mjesto na kojem se u Uniji donose odluke o mjerama upravljanja kibersigurnosnim rizicima. To

Izmjena

(64) Kako bi se u obzir uzela prekogranična priroda usluga i aktivnosti pružatelja DNS usluga, registara naziva vršnih domena, pružatelja mreža za isporuku sadržaja, pružatelja usluga računalstva u oblaku, pružatelja usluga podatkovnog centra i pružatelja digitalnih usluga, samo bi jedna država članica trebala imati nadležnost nad tim subjektima. **U svrhu ove Direktive**, nadležnost bi se trebala dodijeliti državi članici u kojoj predmetni subjekt ima glavni poslovni nastan u Uniji. Kriterij poslovnog nastana za potrebe ove Direktive podrazumijeva učinkovito obavljanje djelatnosti putem stabilnih aranžmana. Pravni oblik takvih aranžmana, bilo kroz podružnicu bilo društvo kćer s pravnom osobnošću, nije odlučujući čimbenik u tom pogledu. Ispunjene tog kriterija ne bi trebalo ovisiti o tome jesu li mrežni i informacijski sustavi fizički smješteni na određenom mjestu; postojanje i upotreba takvih sustava sami po sebi ne čine takav glavni poslovni nastan i stoga nisu odlučujući kriteriji za određivanje glavnog poslovnog nastana. Glavni poslovni nastan trebao bi biti mjesto na kojem se u Uniji donose odluke o mjerama

će obično odgovarati mjestu u Uniji na kojem se nalazi središnja uprava poduzeća. Ako se takve odluke ne donose u Uniji, trebalo bi smatrati da se glavni poslovni nastan nalazi u državama članicama u kojima subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. Ako usluge pruža grupa poduzeća, glavni poslovni nastan vladajućeg poduzeća trebao bi se smatrati glavnim nastanom grupe poduzeća.

upravljanja kibersigurnosnim rizicima. To će obično odgovarati mjestu u Uniji na kojem se nalazi središnja uprava poduzeća. Ako se takve odluke ne donose u Uniji, trebalo bi smatrati da se glavni poslovni nastan nalazi u državama članicama u kojima subjekt ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji. Ako usluge pruža grupa poduzeća, glavni poslovni nastan vladajućeg poduzeća trebao bi se smatrati glavnim nastanom grupe poduzeća.

Amandman 39

Prijedlog direktive Uvodna izjava 69.

Tekst koji je predložila Komisija

(69) Obrada osobnih podataka u mjeri koja je nužna i proporcionalna za potrebe osiguravanja mrežne i informacijske sigurnosti, koju provode subjekti, javna tijela, CERT-ovi, CSIRT-ovi i pružatelji sigurnosnih tehnologija i usluga, trebala bi *se smatrati legitimnim interesom predmetnog* voditelja obrade podataka u *skladu s Uredbom (EU) 2016/679*. To bi trebalo uključivati mjere za sprečavanje, otkrivanje, analizu i odgovor na incidente, mjere za informiranje o određenim kiberprijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim incidentima, kiberprijetnjama i ranjivostima, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate. Takve mjere mogu zahtijevati obradu *sljedećih vrsta* osobnih podataka: IP *adresa, jedinstvenih lokatora* resursa (*URL-ova*), *naziva* domena i *adresa elektroničke pošte*.

Izmjena

(69) Obrada osobnih podataka u mjeri koja je nužna i proporcionalna za potrebe osiguravanja mrežne i informacijske sigurnosti, koju provode subjekti, javna tijela, CERT-ovi, CSIRT-ovi i pružatelji sigurnosnih tehnologija i usluga *potrebna im je za ispunjavanje pravnih obveza u skladu s nacionalnim pravom u koje se prenosi ova Direktiva te je stoga obuhvaćena člankom 6. stavkom 1. točkom (c) i člankom 6. stavkom 3. Uredbe (EU) 2016/679. Nadalje, takva obrada* trebala bi *predstavljati legitiman interes dotičnog* voditelja obrade podataka, *kako je navedeno u članku 6. stavku 1. točki (f) Uredbe (EU) 2016/679*. To bi trebalo uključivati mjere za sprečavanje, otkrivanje, analizu i odgovor na incidente, mjere za informiranje o određenim kiberprijetnjama, razmjenu informacija u kontekstu uklanjanja i koordiniranog otkrivanja ranjivosti, kao i dobrovoljnu razmjenu informacija o tim incidentima, kiberprijetnjama i ranjivostima, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate. *U mnogim slučajevima osobni su podaci ugroženi*

nakon kiberincidenata te bi stoga nadležna tijela i tijela za zaštitu podataka država članica EU-a trebala surađivati i razmjenjivati informacije o svim relevantnim pitanjima radi rješavanja svih povreda osobnih podataka. Takve mjere mogu zahtijevati obradu **određenih kategorija** osobnih podataka, **uključujući IP adresu, jedinstvene lokatore resursa (URL-ove), nazive domena i adresu elektroničke pošte.**

Amandman 40

Prijedlog direktive Uvodna izjava 71.

Tekst koji je predložila Komisija

(71) Kako bi provedba bila učinkovita, potrebno je utvrditi popis minimalnih administrativnih sankcija za kršenje obveza upravljanja kibersigurnosnim rizicima i izvješćivanja predviđenih ovom Direktivom, čime bi se uspostavio jasan i usklađen okvir za takve sankcije širom Unije. Posebna bi se pozornost trebala posvetiti **prirodi**, ozbiljnosti i trajanju povrede, stvarno prouzročenoj šteti ili nastalim gubicima ili potencijalnoj šteti ili gubicima, namjernom ili nehotičnom obilježju povrede, mjerama poduzetima radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka, stupnju odgovornosti ili svim relevantnim prethodnim povredama, stupnju suradnje s nadležnim tijelom kao i bilo kojem drugom otegotnom ili olakotnom čimbeniku. **Izricanje sankcija**, uključujući upravne novčane kazne, trebalo bi podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu i zakonito postupanje.

Izmjena

(71) Kako bi provedba bila učinkovita, potrebno je utvrditi popis minimalnih administrativnih sankcija za kršenje obveza upravljanja kibersigurnosnim rizicima i izvješćivanja predviđenih ovom Direktivom, čime bi se uspostavio jasan i usklađen okvir za takve sankcije širom Unije. Posebna bi se pozornost trebala posvetiti **ozbiljnosti** i trajanju povrede, stvarno prouzročenoj šteti ili nastalim gubicima ili potencijalnoj šteti ili gubicima, namjernom ili nehotičnom obilježju povrede, **eventualnim prethodnim kršenjima, načinu na koji je kršenje postalo poznato nadležnom tijelu** mjerama poduzetima radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka, stupnju odgovornosti ili svim relevantnim prethodnim povredama, stupnju suradnje s nadležnim tijelom kao i bilo kojem drugom otegotnom ili olakotnom čimbeniku. **Nametnute sankcije**, uključujući upravne novčane kazne, trebale bi podlijegati odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu i zakonito postupanje.

Amandman 41

Prijedlog direktive Uvodna izjava 74.

Tekst koji je predložila Komisija

(74) Države članice trebale bi moći propisati pravila o kaznenim sankcijama za povrede nacionalnih pravila kojima se prenosi ova Direktiva. Međutim, izricanje kaznenih sankcija za povrede takvih nacionalnih pravila i povezanih administrativnih sankcija ne bi smjelo dovesti do kršenja načela *ne bis in idem*, kako ga tumači Sud.

Izmjena

(74) Države članice trebale bi moći propisati pravila o kaznenim sankcijama za povrede nacionalnih pravila kojima se prenosi ova Direktiva. ***Te kaznene sankcije mogu obuhvaćati i oduzimanje dobiti stečene kršenjem ove Uredbe.*** Međutim, izricanje kaznenih sankcija za povrede takvih nacionalnih pravila i povezanih administrativnih sankcija ne bi smjelo dovesti do kršenja načela *ne bis in idem*, kako ga tumači Sud.

Amandman 42

Prijedlog direktive Uvodna izjava 76.

Tekst koji je predložila Komisija

(76) Kako bi se dodatno ojačali učinkovitost i odvraćajući učinak sankcija koje se primjenjuju na povrede obveza utvrđenih u skladu s ovom Direktivom, nadležna tijela trebala bi biti ovlaštena za primjenu sankcija koje se sastoje od suspenzije certifikata ili ovlaštenja za dio usluga ili sve usluge koje pruža ključni subjekt i izricanja privremene zabrane fizičkoj osobi da obavlja rukovoditeljske dužnosti. S obzirom na njihovu ozbiljnost i učinak na aktivnosti subjekata te napoljetku na njihove potrošače, takve bi se sankcije trebale primjenjivati samo razmjerno ozbiljnosti povrede i uzimajući u obzir posebne okolnosti svakog slučaja, uključujući namjerna ili nehotična obilježja povrede, kao i mjere poduzete radi sprečavanja ili ublažavanja pretrpljene štete i/ili gubitaka. Takve bi se sankcije

Izmjena

(Ne odnosi se na hrvatsku verziju.)

trebale primjenjivati samo kao ultima ratio, što znači tek nakon što se iscrpe druge odgovarajuće provedbene mjere utvrđene ovom Direktivom i samo dok subjekti na koje se primjenjuju ne poduzmu potrebne mjere za otklanjanje nedostataka ili dok ne ispune zahtjeve nadležnog tijela na koje se odnose te sankcije. Izricanje takvih sankcija podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s općim načelima prava Unije i Poveljom Europske unije o temeljnim pravima, uključujući djelotvornu sudsku zaštitu, zakonito postupanje, prepostavku nedužnosti i pravo na obranu.

Amandman 43

Prijedlog direktive Uvodna izjava 77.

Tekst koji je predložila Komisija

(77) Ovom bi se Direktivom trebala utvrditi pravila suradnje između nadležnih tijela i nadzornih tijela u skladu s Uredbom (EU) 2016/679 radi postupanja u slučaju povreda povezanih s osobnim podacima.

Izmjena

(77) Ovom bi se Direktivom trebala utvrditi pravila suradnje između nadležnih tijela ***u okviru ove Direktive*** i nadzornih tijela u skladu s Uredbom (EU) 2016/679 radi postupanja u slučaju povreda povezanih s osobnim podacima.

Amandman 44

Prijedlog direktive Uvodna izjava 79.

Tekst koji je predložila Komisija

(79) Trebalo bi uvesti mehanizam istorazinskog ocjenjivanja kojim bi se stručnjacima koje su imenovale države članice omogućila procjena provedbe kibersigurnosnih politika, uključujući razinu sposobnosti i dostupnih resursa država članica.

Izmjena

(79) Trebalo bi uvesti mehanizam istorazinskog ocjenjivanja kojim bi se stručnjacima koje su imenovale države članice omogućila procjena provedbe kibersigurnosnih politika, uključujući razinu sposobnosti i dostupnih resursa država članica. ***EU bi trebao olakšati koordinirani odgovor na kiberincidente i kiberkrize velikih razmjera te ponuditi***

*pomoć kako bi se pomoglo povratku
nakon takvih kibernapada.*

Amandman 45

Prijedlog direktive Uvodna izjava 82.a (nova)

Tekst koji je predložila Komisija

Izmjena

(82 a) Ova se Direktiva ne primjenjuje na institucije, urede, tijela i agencije Unije. Međutim, tijela Unije mogla bi se smatrati ključnim ili važnim subjektima u ovoj Direktivi. Kako bi se uskladenim i homogenim pravilima postigla ujednačena razina zaštite, Komisija bi do 31. prosinca 2022. trebala objaviti zakonodavni prijedlog kako bi institucije, urede, tijela i agencije Unije uključila u okvir za kibersigurnost na razini EU-a.

Amandman 46

Prijedlog direktive Uvodna izjava 84.

Tekst koji je predložila Komisija

Izmjena

(84) Ovom Direktivom poštuju se temeljna prava i načela priznata Poveljom Europske unije o temeljnim pravima, posebno pravo na poštovanje privatnog života i komuniciranja, zaštitu osobnih podataka, slobodu poduzetništva, pravo na vlasništvo, pravo na djelotvoran pravni lijek pred sudom i pravo na saslušanje. Ova Direktiva trebala bi se provoditi u skladu s tim pravima i načelima.

(84) Ovom Direktivom poštuju se temeljna prava i načela priznata Poveljom Europske unije o temeljnim pravima, posebno pravo na poštovanje privatnog života i komuniciranja, zaštitu osobnih podataka, slobodu poduzetništva, pravo na vlasništvo, pravo na djelotvoran pravni lijek pred sudom i pravo na saslušanje. Ova Direktiva trebala bi se provoditi u skladu s tim pravima i načelima *te potpuno poštujući postojeće zakonodavstvo Unije u reguliraju tih pitanja. Svaka obrada osobnih podataka na temelju ove Direktive podliježe Uredbi (EU) 2016/679 i Direktivi 2002/58/EZ, u njihovu području primjene, uključujući zadaće i ovlasti nadzornih tijela nadležnih za*

pranje usklađenosti s tim pravnim instrumentima.

Amandman 47

Prijedlog direktive

Članak 2. – stavak 1.

Tekst koji je predložila Komisija

1. Ova se Direktiva primjenjuje na vrste javnih i privatnih subjekata koje se u Prilogu I. navode kao ključni subjekti i u Prilogu II. kao važni subjekti. Ova se Direktiva ne primjenjuje na subjekte koji se smatraju mikropoduzećima i malim poduzećima u smislu **Preporuke** Komisije 2003/361/EZ.²⁸

Izmjena

1. Ova se Direktiva primjenjuje na vrste javnih i privatnih subjekata koje se u Prilogu I. navode kao ključni subjekti i u Prilogu II. kao važni subjekti. Ova se Direktiva ne primjenjuje na subjekte koji se smatraju mikropoduzećima i malim poduzećima u smislu Preporuke Komisije 2003/361/EZ.²⁸ i **članka 3. stavka 4.**

**Priloga Preporuci Komisije
2003/361/EZ.**²⁸

²⁸ Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

²⁸ Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

Amandman 48

Prijedlog direktive

Članak 2. – stavak 2. – uvodni dio

Tekst koji je predložila Komisija

2. Međutim, Direktiva se primjenjuje i na subjekte iz priloga I. i II. neovisno o njihovoj veličini:

Izmjena

2. Međutim, Direktiva se primjenjuje i na subjekte iz priloga I. i II. neovisno o njihovoj veličini **i na temelju ocjene rizika prema članku 18.:**

Amandman 49

Prijedlog direktive

Članak 2. – stavak 2. – točka c

Tekst koji je predložila Komisija

(c) ako je subjekt jedini pružatelj usluge **u državi članici**;

Izmjena

(c) ako je subjekt jedini pružatelj usluge **na nacionalnoj ili regionalnoj razini**;

Amandman 50

Prijedlog direktive

Članak 2. – stavak 2. – točka d

Tekst koji je predložila Komisija

(d) ako bi **mogući** prekid usluge koju pruža subjekt mogao utjecati na javnu sigurnost, javnu zaštitu ili javno zdravlje;

Izmjena

(d) ako bi prekid usluge koju pruža subjekt mogao utjecati na javnu sigurnost, javnu zaštitu ili javno zdravlje;

Amandman 51

Prijedlog direktive

Članak 2. – stavak 2. – točka e

Tekst koji je predložila Komisija

(e) ako bi **mogući** prekid usluge koju pruža subjekt mogao prouzročiti sistemske rizike, posebno u sektorima u kojima bi takav prekid mogao imati prekogranični učinak;

Izmjena

(e) ako bi prekid usluge koju pruža subjekt mogao prouzročiti sistemske rizike, posebno u sektorima u kojima bi takav prekid mogao imati prekogranični učinak;

Amandman 52

Prijedlog direktive

Članak 2. – stavak 4.a (novi)

Tekst koji je predložila Komisija

Izmjena

4a. *Svaka obrada osobnih podataka u skladu s ovom Direktivom mora biti u skladu s Uredbom (EU) 2016/679 i Direktivom 2002/58/EZ i ograničena je na ono što je strogo nužno i razmjerno za potrebe ove Direktive.*

Amandman 53

**Prijedlog direktive
Članak 2. – stavak 5.**

Tekst koji je predložila Komisija

5. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije i nacionalnim pravilima, kao što su pravila o poslovnoj tajni, ustupaju se Komisiji i drugim relevantnim tijelima samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je *relevantno i razmijerno svrhi* te razmjene. Pri razmjeni informacija čuva se njihova povjerljivost te se štite sigurnost i komercijalni interesi ključnih ili važnih subjekata.

Izmjena

5. Ne dovodeći u pitanje članak 346. UFEU-a, informacije koje se smatraju povjerljivima u skladu s pravilima Unije i nacionalnim pravilima, kao što su pravila o poslovnoj tajni, ustupaju se Komisiji i drugim relevantnim tijelima samo u slučaju kad je takva razmjena nužna za primjenu ove Direktive. Razmijenjene informacije ograničuju se na ono što je **nužno za svrhu** te razmjene. Pri razmjeni informacija čuva se njihova povjerljivost te se štite sigurnost i komercijalni interesi ključnih ili važnih subjekata.

Amandman 54

**Prijedlog direktive
Članak 2. – stavak 6.a (novi)**

Tekst koji je predložila Komisija

Izmjena

6 a. Komisija prije 31. prosinca 2021. objavljuje zakonodavni prijedlog za uključivanje institucija, ureda, tijela i agencija Unije u sveukupni okvir za kibersigurnost na razini EU-a u cilju postizanja ujednačene razine zaštite dosljednim i homogenim pravilima.

Amandman 55

**Prijedlog direktive
Članak 4. – stavak 1. – točka 1. – podtočka b**

Tekst koji je predložila Komisija

Izmjena

(b) svaki uređaj ili skupina povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka;

(b) svaki uređaj ili skupina povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka *i koji su integrirani u IT sustave koji se koriste za pružanje njihovih usluga;*

Amandman 56

Prijedlog direktive Članak 4. – stavak 1. – točka 4.

Tekst koji je predložila Komisija

(4) „nacionalna strategija za kibersigurnost” znači usklađen okvir države članice kojim se predviđaju strateški ciljevi i prioriteti za **sigurnost mrežnih i informacijskih sustava** u toj državi članici;

Izmjena

(4) „nacionalna strategija za kibersigurnost” znači usklađen okvir države članice kojim se predviđaju strateški ciljevi i prioriteti za **kibersigurnost** u toj državi članici;

Amandman 57

Prijedlog direktive Članak 4. – stavak 1. – točka 12.

Tekst koji je predložila Komisija

(12) „središte za razmjenu internetskog prometa (IXP)” znači mrežni instrument koji omogućuje međusobno povezivanje više od dviju neovisnih mreža (autonomnih sustava), prvenstveno u svrhu olakšavanja razmjene internetskog prometa; IXP omogućuje međusobno povezivanje samo za autonomne sustave; za IXP nije potrebno da internetski promet između bilo kojih dvaju autonomnih sustava sudionika prođe kroz bilo koji treći autonomni sustav, on takav promet ne mijenja i ne utječe na njega ni na koji drugi način;

Izmjena

Briše se.

Amandman 58

Prijedlog direktive Članak 4. – stavak 1. – točka 22.

Tekst koji je predložila Komisija

(22) „platforma za usluge društvenih mreža” znači platforma koja krajnjim korisnicima omogućuje da se međusobno povežu, dijele i otkrivaju sadržaj te da

Izmjena

Briše se.

komuniciraju na više uređaja, a posebno putem razgovora, objava, videozapisa i preporuka;

Amandman 59

Prijedlog direktive

Članak 4. – stavak 1. – točka 24.

Tekst koji je predložila Komisija

(24) „subjekt” znači svaka fizička ili pravna osoba osnovana i priznata kao takva na temelju nacionalnog prava mjesa svojeg poslovnog nastana, koja može, djelujući u vlastito ime, ostvarivati prava i preuzimati obveze; „ključni subjekt” znači svaka vrsta subjekta koja se Prilogu I. navodi kao ključni subjekt;

Izmjena

(24) „subjekt” znači svaka fizička **osoba** ili **svaka** pravna osoba osnovana i priznata kao takva na temelju nacionalnog prava mjesa svojeg poslovnog nastana, koja može, djelujući u vlastito ime, ostvarivati prava i preuzimati obveze;

Amandman 60

Prijedlog direktive

Članak 5. – stavak 1. – točka a

Tekst koji je predložila Komisija

(a) definiciju ciljeva i prioriteta strategije država članica za kibersigurnost;

Izmjena

(a) definiciju ciljeva i prioriteta strategije država članica za kibersigurnost, *uzimajući u obzir opću razinu osviještenosti građana o kibersigurnosti, kao i opću razinu sigurnosti uređaja povezanih s potrošačima;*

Amandman 61

Prijedlog direktive

Članak 5. – stavak 1. – točka f

Tekst koji je predložila Komisija

(f) okvir politike za bolju koordinaciju između nadležnih tijela iz ove Direktive i Direktive (EU) XXXX/XXXX Europskog parlamenta i Vijeća³⁸ [Direktiva o

Izmjena

(f) okvir politike za bolju koordinaciju između nadležnih tijela iz ove Direktive i Direktive (EU) XXXX/XXXX Europskog parlamenta i Vijeća³⁸ [Direktiva o

otpornosti kritičnih subjekata] u svrhu razmjene informacija o incidentima i kiberprijetnjama te izvršavanja nadzornih zadaća.

³⁸ [Upisati puni naslov i upućivanje na objavu u SL-u kada budu poznati.]

Amandman 62

Prijedlog direktive Članak 5. – stavak 2. – točka b

Tekst koji je predložila Komisija

(b) smjernice za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i usluge u području javne nabave;

Izmjena

(b) smjernice za uključivanje i definiranje kibersigurnosnih zahtjeva za IKT proizvode i usluge u području javne nabave, *što uključuje, ali nije ograničeno na zahtjeve za šifriranje i promicanje upotrebe proizvoda za kibersigurnost otvorenog koda;*

Amandman 63

Prijedlog direktive Članak 5. – stavak 2. – točka da (nova)

Tekst koji je predložila Komisija

Izmjena

(da) politiku koja se odnosi na jamčenje daljnje upotrebe otvorenih podataka i otvorenog koda kako bi se osigurala sigurnosti na temelju transparentnosti;

Amandman 64

Prijedlog direktive Članak 5. – stavak 2. – točka db (nova)

Tekst koji je predložila Komisija

Izmjena

(db) politiku kojom se promiču privatnost i sigurnost osobnih podataka korisnika internetskih usluga;

Amandman 65

Prijedlog direktive Članak 5. – stavak 2. – točka e

Tekst koji je predložila Komisija

(e) politiku promicanja i razvoja vještina u području kibersigurnosti, informiranja te istraživačkih i razvojnih inicijativa;

Izmjena

(e) politiku promicanja i razvoja vještina u području kibersigurnosti, informiranja te istraživačkih i razvojnih inicijativa, *uključujući razvoj programa osposobljavanja u području kibersigurnosti kako bi se subjektima pružili stručnjaci i tehničari*;

Amandman 66

Prijedlog direktive Članak 5. – stavak 2. – točka f

Tekst koji je predložila Komisija

(f) politiku potpore akademskim i istraživačkim institucijama *u razvoju* alata za kibersigurnost i sigurne mrežne infrastrukture;

Izmjena

(f) politiku potpore akademskim i istraživačkim institucijama *koje doprinose nacionalnoj strategiji za kibersigurnost razvojem i uvođenjem* alata za kibersigurnost i sigurne mrežne infrastrukture *kojima se doprinosi nacionalnoj strategiji kibersigurnosti, uključujući posebne politike za rješavanje pitanja rodne zastupljenosti i ravnoteže u tom sektoru*;

Amandman 67

Prijedlog direktive Članak 5. – stavak 2. – točka h

Tekst koji je predložila Komisija

(h) politiku za rješavanje posebnih potreba MSP-ova, osobito onih izuzetih iz područja primjene ove Direktive, u pogledu smjernica i potpore za poboljšanje

Izmjena

(h) politiku za rješavanje posebnih potreba MSP-ova, osobito onih izuzetih iz područja primjene ove Direktive, u pogledu smjernica i potpore za poboljšanje njihove otpornosti na kiberprijetnje *i*

njihove otpornosti na kiberprijetnje.

njihovog kapaciteta da odgovore na kirbersigurnosne incidente.

Amandman 68

Prijedlog direktive

Članak 6. – stavak 2.

Tekst koji je predložila Komisija

2. ENISA razvija i vodi europski registar ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke osobito kako bi omogućila važnim i ključnim subjektima, kao i njihovim dobavljačima mrežnih i informacijskih sustava da otkriju i registriraju ranjivosti prisutne u IKT proizvodima ili IKT uslugama te da svim zainteresiranim stranama omoguće pristup informacijama o ranjivostima sadržanima u registru. Registar konkretno uključuje informacije o ranjivosti, IKT proizvodu ili IKT uslugama na koje ona utječe i ozbiljnosti ranjivosti s obzirom na okolnosti u kojima se može iskoristiti, dostupnosti odgovarajućih popravaka i, ako nisu dostupni, smjernica namijenjenih korisnicima ranjivih proizvoda i usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti.

Izmjena

2. ENISA razvija i vodi europski registar ranjivosti. U tu svrhu ENISA uspostavlja i održava odgovarajuće informacijske sustave, politike i postupke osobito kako bi omogućila važnim i ključnim subjektima, kao i njihovim dobavljačima mrežnih i informacijskih sustava da otkriju i registriraju ranjivosti prisutne u IKT proizvodima ili IKT uslugama te da svim zainteresiranim stranama omoguće pristup informacijama o ranjivostima sadržanima u registru. Registar konkretno uključuje informacije o ranjivosti, IKT proizvodu ili IKT uslugama na koje ona utječe i ozbiljnosti ranjivosti s obzirom na okolnosti u kojima se može iskoristiti, dostupnosti odgovarajućih popravaka i, ako nisu dostupni, smjernica namijenjenih korisnicima ranjivih proizvoda i usluga o načinu na koji se mogu ublažiti rizici koji proizlaze iz otkrivenih ranjivosti. *Kako bi se osigurala sigurnost i dostupnost informacija sadržanih u registru, ENISA primjenjuje najnovije sigurnosne mjere i stavlja ih na raspolaganje u strojno čitljivim formatima putem odgovarajućih sučelja.*

Amandman 69

Prijedlog direktive

Članak 7. – stavak 3. – točka a

Tekst koji je predložila Komisija

(a) ciljevi mjera i aktivnosti *za*

Izmjena

(a) ciljevi *nacionalnih i, ako je*

nacionalnu pripravnost;

relevantno i primjenjivo, regionalnih i prekograničnih mjera i aktivnosti pripravnosti;

Amandman 70

Prijedlog direktive Članak 10. – stavak 2. – točka e

Tekst koji je predložila Komisija

(e) osiguravanje, na zahtjev subjekta, *proaktivnog pregledavanja mrežnih* i informacijskih sustava koji se upotrebljavaju za pružanje njihovih usluga;

Izmjena

(e) osiguravanje, na zahtjev subjekta, *sigurnosnog pregleda* informacijskih sustava i *mrežnog dometa* koji se upotrebljavaju za pružanje njihovih usluga; *kako bi se prepoznale, ublažile ili spriječile specifične prijetnje; obrada osobnih podataka u okviru takvog pregledavanja ograničena je na strogo neophodno, a svakako na IP adresu i URL-ove.*

Amandman 71

Prijedlog direktive Članak 11. – stavak 4.

Tekst koji je predložila Komisija

4. U mjeri u kojoj je to potrebno za učinkovito izvršavanje zadaća i obveza utvrđenih u ovoj Direktivi, države članice osiguravaju odgovarajuću suradnju između nadležnih tijela i jedinstvenih kontaktnih točaka i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka i tijela odgovornih za kritičnu infrastrukturu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] i nacionalnih finansijskih tijela imenovanih u skladu s Uredbom (EU) XXXX/XXXX Europskog parlamenta i Vijeća³⁹ [Uredba DORA] unutar te države članice.

Izmjena

4. U mjeri u kojoj je to potrebno za učinkovito izvršavanje zadaća i obveza utvrđenih u ovoj Direktivi, države članice osiguravaju odgovarajuću suradnju između nadležnih tijela i jedinstvenih kontaktnih točaka i tijela za izvršavanje zakonodavstva, tijela za zaštitu podataka i tijela odgovornih za kritičnu infrastrukturu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] i nacionalnih finansijskih tijela imenovanih u skladu s Uredbom (EU) XXXX/XXXX Europskog parlamenta i Vijeća³⁹ [Uredba DORA] unutar te države članice **u skladu s njihovim nadležnostima.**

³⁹ [Upisati puni naslov i upućivanje na

³⁹ [Upisati puni naslov i upućivanje na

objavu u SL-u kada budu poznati.]

objavu u SL-u kada budu poznati.]

Amandman 72

Prijedlog direktive Članak 11. – stavak 5.

Tekst koji je predložila Komisija

5. Države članice osiguravaju da njihova nadležna tijela redovito dostavljaju informacije nadležnim tijelima imenovanim u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] o kibersigurnosnim rizicima, kiberprijetnjama i incidentima koji utječu na ključne subjekte koji su utvrđeni kao kritični ili kao subjekti istovjetni kritičnim subjektima, u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti ključnih subjekata], kao i o mjerama koje su nadležna tijela poduzela kao odgovor na te rizike i incidente.

Izmjena

5. Države članice osiguravaju da njihova nadležna tijela redovito dostavljaju **pravovremene** informacije nadležnim tijelima imenovanim u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] o kibersigurnosnim rizicima, kiberprijetnjama i incidentima koji utječu na ključne subjekte koji su utvrđeni kao kritični ili kao subjekti istovjetni kritičnim subjektima, u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti ključnih subjekata], kao i o mjerama koje su nadležna tijela poduzela kao odgovor na te rizike i incidente.

Amandman 73

Prijedlog direktive Članak 12. – stavak 3. – uvodni dio

Tekst koji je predložila Komisija

3. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e. Europska služba za vanjsko djelovanje **sudjeluje** u aktivnostima skupine za suradnju kao **promatrač**. Europska nadzorna tijela u skladu s člankom 17. stavkom 5. točkom (c) Uredbe (EU) XXXX/XXXX [Uredba DORA] mogu sudjelovati u aktivnostima skupine za suradnju.

Izmjena

3. Skupina za suradnju sastoji se od predstavnika država članica, Komisije i ENISA-e. Europska služba za vanjsko djelovanje, **Europski centar za kibernetički kriminal pri Europolu i Europski odbor za zaštitu podataka sudjeluju** u aktivnostima skupine za suradnju kao **promatrači**. Europska nadzorna tijela u skladu s člankom 17. stavkom 5. točkom (c) Uredbe (EU) XXXX/XXXX [Uredba DORA] mogu sudjelovati u aktivnostima skupine za suradnju.

Amandman 74

Prijedlog direktive Članak 12. – stavak 3. – podstavak 1.

Tekst koji je predložila Komisija

Skupina za suradnju **može, prema potrebi, pozvati** predstavnike relevantnih dionika da sudjeluju u njezinu radu.

Izmjena

Ako je to relevantno za obavljanje njezinih zadaća, Skupina za suradnju poziva predstavnike relevantnih dionika da sudjeluju u njezinu radu, a Europski parlament da sudjeluje kao promatrač.

Amandman 75

Prijedlog direktive Članak 12. – stavak 8.

Tekst koji je predložila Komisija

8. Skupina za suradnju sastaje se redovito, a najmanje **jednom** godišnje, sa skupinom za otpornost kritičnih subjekata osnovanom na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] radi **promicanja** strateške suradnje i razmjene informacija.

Izmjena

8. Skupina za suradnju sastaje se redovito, a najmanje **dvaput** godišnje, sa skupinom za otpornost kritičnih subjekata osnovanom na temelju Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] radi **olakšavanja** strateške suradnje i razmjene informacija **u stvarnom vremenu**.

Amandman 76

Prijedlog direktive Članak 13. – stavak 2.

Tekst koji je predložila Komisija

2. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova država članica i CERT-EU-a. Komisija u mreži CSIRT-ova **sudjeluje** kao **promatrač**. ENISA osigurava tajništvo i aktivno podržava suradnju među CSIRT-ovima.

Izmjena

2. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova država članica i CERT-EU-a. Komisija i **Europski centar za kiberkriminalitet pri Europolu** u mreži CSIRT-ova **sudjeluju** kao **promatrači**. ENISA osigurava tajništvo i aktivno podržava suradnju među CSIRT-ovima.

Amandman 77

Prijedlog direktive

Članak 14. – stavak 2.

Tekst koji je predložila Komisija

2. EU-CyCLONe čine predstavnici tijela država članica za upravljanje krizama koja su imenovana u skladu s člankom 7., Komisija i ENISA. ENISA osigurava tajništvo mreže i podupire sigurnu razmjenu informacija.

Izmjena

2. EU-CyCLONe čine predstavnici tijela država članica za upravljanje krizama koja su imenovana u skladu s člankom 7., Komisija i ENISA. *Europski centar za kiberkriminalitet pri Europolu sudjeluje u aktivnostima mreže organizacija EU-CyCLONe kao promatrač.* ENISA osigurava tajništvo mreže i podupire sigurnu razmjenu informacija.

Amandman 78

Prijedlog direktive

Članak 14. – stavak 6.

Tekst koji je predložila Komisija

6. EU-CyCLONe surađuje s mrežom CSIRT-ova na temelju dogovorenih postupovnih aranžmana.

Izmjena

6. EU-CyCLONe surađuje s mrežom CSIRT-ova na temelju dogovorenih postupovnih aranžmana *te s tijelima za kazneni progon u okviru protokola za odgovor tijelâ kaznenog progona na krizne situacije EU-a.*

Amandman 79

Prijedlog direktive

Članak 15. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. ENISA u suradnji s Komisijom izdaje *dvogodišnje* izvješće o stanju kibersigurnosti u Uniji. *Izvješćem* je posebno obuhvaćena ocjena sljedećeg:

Izmjena

1. ENISA u suradnji s Komisijom izdaje *godišnje* izvješće o stanju kibersigurnosti u Uniji. *Izvješće se dostavlja u strojno čitljivom formatu te je njime* posebno obuhvaćena ocjena sljedećeg:

Amandman 80

Prijedlog direktive

Članak 15. – stavak 1. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(ca) učinak kiberincidenata na zaštitu osobnih podataka u Uniji.

Amandman 81

Prijedlog direktive

Članak 15. – stavak 1. – točka cb (nova)

Tekst koji je predložila Komisija

Izmjena

(cb) pregleda opće razine osviještenosti o kibersigurnosti i njezine upotrebe među građanima te opće razine sigurnosti povezanih uredaja koji su namijenjeni potrošačima na tržištu Unije;

Amandman 82

Prijedlog direktive

Članak 17. – stavak 2.

Tekst koji je predložila Komisija

Izmjena

2. Države članice osiguravaju da članovi upravljačkog tijela redovito pohađaju posebna ospozobljavanja kako bi stekli dovoljno znanja i vještina za razumijevanje i procjenu kibersigurnosnih rizika i praksi upravljanja, kao i njihova učinka na poslovanje subjekta.

2. Države članice osiguravaju da članovi upravljačkog tijela *i specijalisti odgovorni za kibersigurnost* redovito pohađaju posebna ospozobljavanja kako bi stekli dovoljno znanja i vještina za razumijevanje i procjenu kibersigurnosnih rizika *koji evoluiraju* i praksi upravljanja, kao i njihova učinka na poslovanje subjekta.

Amandman 83

Prijedlog direktive

Članak 18. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere upravljanja rizicima

1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke i organizacijske mjere upravljanja rizicima

kojima su izloženi mrežni i informacijski sustavi kojima se *ti subjekti* služe u pružanju svojih usluga. Uzimajući u obzir najnovija dostignuća, tim se mjerama osigurava razina *sigurnosti* mrežnih i informacijskih sustava koja odgovara postojećem riziku.

za kibersigurnost kojima su izloženi mrežni i informacijski sustavi kojima se služe u pružanju svojih usluga *te radi osiguravanja kontinuiteta tih usluga i upravljanja rizicima kojima su izložena prava pojedinaca pri obradi njihovih osobnih podataka*. Uzimajući u obzir najnovija dostignuća, tim se mjerama osigurava razina *kibersigurnosti* mrežnih i informacijskih sustava koja odgovara postojećem riziku.

Amandman 84

Prijedlog direkitive

Članak 18. – stavak 2. – točka g

Tekst koji je predložila Komisija

(g) primjenu kriptografije i šifriranja.

Izmjena

(g) primjenu kriptografije i *snažnog* šifriranja.

Amandman 85

Prijedlog direkitive

Članak 18. – stavak 3.

Tekst koji je predložila Komisija

3. Države članice osiguravaju da subjekti pri razmatranju odgovarajućih mjera iz stavka 2. točke (d) uzimaju u obzir ranjivosti specifične za svakog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke.

Izmjena

3. Države članice osiguravaju da subjekti pri razmatranju odgovarajućih *razmjernih* mjera iz stavka 2. točke (d) uzimaju u obzir ranjivosti specifične za svakog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibersigurnosnu praksu svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke. *Nadležna tijela subjektima pružaju smjernice o praktičnoj i razmjernej primjeni.*

Amandman 86

Prijedlog direkitive

Članak 18. – stavak 6.a (novi)

Tekst koji je predložila Komisija

Izmjena

6.a Države članice korisniku mrežnog i informacijskog sustava koji pruža ključan ili važan subjekt daju pravo da od subjekta dobiju informacije o postojećim tehničkim i organizacijskim mjerama za upravljanje rizicima za sigurnost mrežnih i informacijskih sustava. Države članice utvrđuju ograničenja tog prava.

Amandman 87

Prijedlog direktive Članak 19. – stavak 1.

Tekst koji je predložila Komisija

1. Skupina za suradnju, zajedno s Komisijom i ENISA-om, **može provoditi** koordinirane procjene sigurnosnih rizika za određene ključne lance opskrbe IKT uslugama, sustavima ili proizvodima, uzimajući u obzir tehničke i, prema potrebi, netehničke čimbenike rizika.

Izmjena

1. Skupina za suradnju, zajedno s Komisijom i ENISA-om, **provodi** koordinirane procjene sigurnosnih rizika za određene ključne lance opskrbe IKT uslugama, sustavima ili proizvodima, uzimajući u obzir tehničke i, prema potrebi, netehničke čimbenike rizika.

Amandman 88

Prijedlog direktive Članak 20. – stavak 1.

Tekst koji je predložila Komisija

1. Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode obavješćuju nadležna tijela ili CSIRT u skladu sa stvcima 3. i 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga. **Prema potrebi**, ti subjekti bez nepotrebne odgode obavješćuju primatelje svojih usluga o incidentima koji bi mogli negativno utjecati na pružanje **tih usluga**. Države članice osiguravaju da ti subjekti, među ostalim, prijavljaju sve informacije koje nadležnim tijelima ili CSIRT-ovima omogućuju da utvrde sve prekogranične učinke incidenta.

Izmjena

1. Države članice osiguravaju da ključni i važni subjekti bez nepotrebne odgode, **a u svakom slučaju u roku od 24 sata**, obavješćuju nadležna tijela ili CSIRT u skladu sa stvcima 3. i 4. o svakom incidentu koji ima znatan učinak na pružanje njihovih usluga, **a nadležna tijela za provedbu zakonodavstva ako se sumnja ili zna da je incident zlonamjerne prirode**. Ti subjekti bez nepotrebne odgode, **a u svakom slučaju u roku od 24 sata**, obavješćuju primatelje svojih usluga o incidentima koji bi mogli negativno utjecati na pružanje **te usluge i pružaju informacije koje bi im omogućile ublažavanje štetnih učinaka kibernapada**.

Iznimno, ako bi javno otkrivanje moglo izazvati daljnje kibernapade, ti subjekti mogu odgoditi obavješćivanje. Države članice osiguravaju da ti subjekti, među ostalim, prijavljuju sve informacije koje nadležnim tijelima ili CSIRT-ovima omogućuju da utvrde sve prekogranične učinke incidenta.

Amandman 89

Prijedlog direktive

Članak 20. – stavak 2. – uvodni dio

Tekst koji je predložila Komisija

2. Države članice osiguravaju da ključni i važni subjekti **bez nepotrebne odgode obavješćuju** nadležna tijela ili CSIRT o svim ozbiljnim kiberprijetnjama za koje ti subjekti utvrde da bi mogle dovesti do ozbiljnog incidenta.

Izmjena

2. Države članice osiguravaju da ključni i važni subjekti **mogu obavijestiti** nadležna tijela ili CSIRT o svim ozbiljnim kiberprijetnjama za koje ti subjekti utvrde da bi mogle dovesti do ozbiljnog incidenta.

Amandman 90

Prijedlog direktive

Članak 20. – stavak 2. – podstavak 1.

Tekst koji je predložila Komisija

Ako je primjenjivo, **ti subjekti bez nepotrebne odgode obavješćuju** primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja o svim mjerama ili pravnim lijekovima koje ti primatelji mogu poduzeti kao odgovor na tu prijetnju.
Prema potrebi, subjekti isto tako obavješćuju te primatelje o samoj prijetnji. Subjekt koji šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.

Izmjena

Ako je primjenjivo, **tim subjektima se dozvoljava da obavijeste** primatelje svojih usluga na koje bi mogla utjecati ozbiljna kiberprijetnja o svim mjerama ili pravnim lijekovima koje ti primatelji mogu poduzeti kao odgovor na tu prijetnju. **Ako to učine**, subjekti isto tako obavješćuju te primatelje o samoj prijetnji. Subjekt koji šalje obavijest ne podliježe zbog toga povećanoj odgovornosti.

Amandman 91

Prijedlog direktive

Članak 20. – stavak 4. – točka c – uvodni dio

Tekst koji je predložila Komisija

(c) **završno** izvješće najkasnije mjesec dana nakon podnošenja obavijesti iz točke (a), koje uključuje najmanje sljedeće:

Izmjena

(c) **sveobuhvatno** izvješće najkasnije mjesec dana nakon podnošenja obavijesti iz točke (a), koje uključuje najmanje sljedeće:

Amandman 92

Prijedlog direktive

Članak 20. – stavak 4. – točka c – podtočka ii.

Tekst koji je predložila Komisija

ii. vrstu **prijetnje** ili temeljnog uzroka koji je vjerojatno prouzročio incident;

Izmjena

ii. vrstu **kiberprijetnje** ili temeljnog uzroka koji je vjerojatno prouzročio incident;

Amandman 93

Prijedlog direktive

Članak 20. – stavak 4. – točka c – podtočka iii.

Tekst koji je predložila Komisija

iii. provedene i tekuće mjere ublažavanja.

Izmjena

iii. provedene i tekuće mjere ublažavanja **ili pravna sredstva**.

Amandman 94

Prijedlog direktive

Članak 20. – stavak 6.

Tekst koji je predložila Komisija

6. Nadležno tijelo ili CSIRT prema potrebi o incidentu obavješćuju ostale pogodjene države članice i ENISA-u, a osobito ako se incident iz stavka 1. odnosi na dvije ili više država članica. Pritom nadležna tijela, CSIRT-ovi i jedinstvene kontaktne točke, u skladu s pravom Unije ili nacionalnim zakonodavstvom usklađenim s pravom Unije, čuvaju sigurnost i komercijalne interese subjekta

Izmjena

6. Nadležno tijelo ili CSIRT prema potrebi o incidentu obavješćuju ostale pogodjene države članice i ENISA-u, a osobito ako se incident iz stavka 1. odnosi na dvije ili više država članica. **Ako se incident odnosi na dvije ili više država članica i ako se sumnja da je kriminalne prirode, nadležno tijelo CSIRT-a o tome obavješćuje EUROPOL**. Pritom nadležna tijela, CSIRT-ovi i jedinstvene kontaktne

te povjerljivost dostavljenih informacija.

točke, u skladu s pravom Unije ili nacionalnim zakonodavstvom usklađenim s pravom Unije, čuvaju sigurnost i komercijalne interese subjekta te povjerljivost dostavljenih informacija.

Amandman 95

Prijedlog direktive Članak 22. – stavak 2.

Tekst koji je predložila Komisija

2. ENISA u suradnji s državama članicama izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.

Izmjena

2. ENISA *nakon savjetovanja s Europskim odborom za zaštitu podataka* u suradnji s državama članicama izrađuje savjete i smjernice u pogledu tehničkih područja koja treba razmotriti u odnosu na stavak 1. te u odnosu na postojeće norme, uključujući nacionalne norme država članica, kojima bi se ta područja mogla obuhvatiti.

Amandman 96

Prijedlog direktive Članak 23. – stavak 1.

Tekst koji je predložila Komisija

1. Kako bi se pridonijelo sigurnosti, stabilnosti i otpornosti DNS-a, države članice osiguravaju da *registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu prikupljaju i održavaju točne i potpune podatke* o registraciji naziva domena u posebnoj bazi podataka *uz dužnu pažnju* u skladu s pravom Unije o zaštiti osobnih podataka.

Izmjena

1. Kako bi se pridonijelo sigurnosti, stabilnosti i otpornosti DNS-a, države članice osiguravaju da *imaju politike i postupke kako bi osigurale prikupljanje i održavanje točnih i potpunih podataka* o registraciji naziva domena u posebnoj bazi podataka skladu s pravom Unije o zaštiti osobnih podataka. *Države članice osiguravaju da su takve politike i postupci javno dostupni.*

Amandman 97

Prijedlog direktive Članak 23. – stavak 2.

Tekst koji je predložila Komisija

2. Države članice osiguravaju da baze podataka o registraciji naziva domena iz stavka 1. sadržavaju **relevantne** informacije za identifikaciju i kontakt nositelja naziva domena te kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena.

Izmjena

2. Države članice osiguravaju da baze podataka o registraciji naziva domena iz stavka 1. sadržavaju informacije **potrebne** za identifikaciju i kontakt nositelja naziva domena, *i to naziv, fizičku i elektroničku adresu te broj telefona* te kontaktnih točaka koje upravljaju nazivima domena u okviru vršnih domena.

Amandman 98

**Prijedlog direktive
Članak 23. – stavak 3.**

Tekst koji je predložila Komisija

3. *Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu uspostave politike i postupke kojima se osigurava da baze podataka sadržavaju točne i potpune informacije. Države članice osiguravaju da su takve politike i postupci javno dostupni.*

Izmjena

Briše se.

Obrazloženje

Ovaj je stavak prenesen u članak 23. stavak 1.

Amandman 99

**Prijedlog direktive
Članak 23. – stavak 4.**

Tekst koji je predložila Komisija

4. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu bez nepotrebne odgode nakon registracije naziva domene objave podatke o registraciji domene *koji*

Izmjena

4. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu *u skladu s člankom 6. stavkom 1. točkom (c) i člankom 6. stavkom 3. Uredbe (EU)*

nisu osobni podaci.

2016/679 bez nepotrebne odgode nakon registracije naziva domene objave *određene* podatke o registraciji *naziva domene poput naziva domene i naziva pravne osobe.*

Amandman 100

Prijedlog direktive Članak 23. – stavak 5.

Tekst koji je predložila Komisija

5. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu omoguće pristup određenim podacima o registraciji naziva domena na temelju zakonitih i opravdanih zahtjeva *legitimnih tražitelja pristupa*, u skladu s pravom Unije o zaštiti podataka. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu bez nepotrebne odgode odgovaraju na sve zahtjeve za pristup. Države članice osiguravaju javnu dostupnost politika i postupaka za objavljivanje takvih podataka.

Izmjena

5. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu omoguće pristup određenim podacima o registraciji naziva domena na temelju zakonitih i opravdanih zahtjeva *javnih tijela, uključujući nadležna tijela u skladu s ovom Direktivom, nadležnih tijela u skladu s pravom Unije ili nacionalnim pravom za sprečavanje, istragu ili progon kaznenih djela ili nadzornih tijela u skladu s Uredbom (EU) 2016/679*, u skladu s pravom Unije o zaštiti podataka. Države članice osiguravaju da registri naziva vršnih domena i subjekti koji pružaju usluge registracije naziva domena za vršnu domenu bez nepotrebne odgode odgovaraju na sve *zakonite i propisno obrazložene* zahtjeve za pristup. Države članice osiguravaju javnu dostupnost politika i postupaka za objavljivanje takvih podataka.

Amandman 101

Prijedlog direktive Članak 24. – stavak 3.

Tekst koji je predložila Komisija

3. Ako subjekt iz stavka 1. nema poslovni nastan u Uniji, ali nudi usluge unutar Unije, dužan je imenovati

Izmjena

3. Ako subjekt iz stavka 1. nema poslovni nastan u Uniji, ali nudi usluge unutar Unije, dužan je imenovati

predstavnika u Uniji. Predstavnik mora imati poslovni nastan u jednoj od država članica u kojima subjekt nudi svoje usluge. Smatra se da takav subjekt pripada nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan. Ako predstavnik unutar Unije nije imenovan u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne mjere protiv subjekta zbog nepoštovanja obveza iz ove Direktive.

predstavnika u Uniji. Predstavnik mora imati poslovni nastan u jednoj od država članica u kojima subjekt nudi svoje usluge.

Ne dovodeći u pitanje nadležnost nadzornih tijela u okviru Uredbe (EU) 2016/679

smatra se da takav subjekt pripada nadležnosti one države članice u kojoj njegov predstavnik ima poslovni nastan. Ako predstavnik unutar Unije nije imenovan u skladu s ovim člankom, svaka država članica u kojoj subjekt pruža usluge može poduzeti pravne mjere protiv subjekta zbog nepoštovanja obveza iz ove Direktive.

Amandman 102

Prijedlog direkture

Članak 25. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. ENISA uspostavlja i vodi register za ključne i važne subjekte iz članka 24. stavka 1. Najkasnije do [12 mjeseci nakon stupanja na snagu ove Direktive] subjekti dostavljaju ENISA-i sljedeće informacije:

Izmjena

1. ENISA uspostavlja i vodi ***siguran*** register za ključne i važne subjekte iz članka 24. stavka 1. Najkasnije do [12 mjeseci nakon stupanja na snagu ove Direktive] subjekti dostavljaju ENISA-i sljedeće informacije:

Amandman 103

Prijedlog direkture

Članak 26. – stavak 1. – uvodni dio

Tekst koji je predložila Komisija

1. Ne dovodeći u pitanje Uredbu (EU) 2016/679, države članice osiguravaju da ključni i važni subjekti mogu međusobno razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kiberprijetnje, ranjivosti, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate, ako takva razmjena informacija:

Izmjena

1. Ne dovodeći u pitanje Uredbu (EU) 2016/679 ***ili Direktivu 2002/58/EZ***, države članice osiguravaju da ključni i važni subjekti mogu međusobno razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kiberprijetnje, ranjivosti, pokazatelje ugroženosti, taktike, tehnike i postupke, kibersigurnosna upozorenja i konfiguracijske alate ***te lokaciju i identitet napadača***, ako takva razmjena informacija:

Amandman 104

Prijedlog direktive Članak 28. – stavak 2.

Tekst koji je predložila Komisija

2. Nadležna tijela blisko surađuju s tijelima **za zaštitu podataka** u rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka.

Izmjena

2. Nadležna tijela blisko surađuju s **nadzornim** tijelima **u** rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka **ne dovodeći u pitanje nadležnosti, zadaće i ovlasti nadzornih tijela u skladu s Uredbom (EU) 2016/679. U tu svrhu nadležna tijela i nadzorna tijela razmjenjuju informacije relevantne za njihovo područje nadležnosti. Nadalje, nadležna tijela na zahtjev nadležnih nadzornih tijela pružaju im sve informacije dobivene u okviru revizija i istraga koje se odnose na obradu osobnih podataka.**

Amandman 105

Prijedlog direktive Članak 29. – stavak 4. – točka h

Tekst koji je predložila Komisija

(h) naložiti tim subjektima da objave aspekte nepoštovanja obveza predviđenih ovom Direktivom na utvrđeni način;

Izmjena

Briše se.

Amandman 106

Prijedlog direktive Članak 29. – stavak 5. – točka b

Tekst koji je predložila Komisija

(b) nametnuti ili zahtijevati da relevantna tijela ili sudovi u skladu s nacionalnim pravom propišu privremenu zabranu obavljanja rukovoditeljskih dužnosti u tom ključnom subjektu svakoj

Izmjena

Briše se.

osobi koja te dužnosti obavlja na razini glavnog izvršnog direktora ili pravnog zastupnika u tom ključnom subjektu te svakoj drugoj fizičkoj osobi koja se smatra odgovornom za povredu.

Amandman 107

Prijedlog direktive

Članak 29. – stavak 5. – podstavak 1.

Tekst koji je predložila Komisija

Te se sankcije primjenjuju samo dok subjekt ne poduzme potrebne mjere za otklanjanje nedostataka ili dok ne ispuni zahtjeve nadležnog tijela za koje su takve sankcije primijenjene.

Izmjena

Ta se sankcija primjenjuje samo dok subjekt ne poduzme potrebne mjere za otklanjanje nedostataka ili dok ne ispuni zahtjeve nadležnog tijela za koje su takve sankcije primijenjene.

Amandman 108

Prijedlog direktive

Članak 29. – stavak 7. – točka c

Tekst koji je predložila Komisija

(c) stvarno prouzročenu štetu ili *nastale gubitke* ili *potencijalnu štetu* ili gubitke, u mjeri u kojoj ih je moguće utvrditi. Pri evaluaciji tog aspekta u obzir se uzimaju, među ostalim, stvarni ili potencijalni finansijski ili gospodarski gubici, učinci na druge usluge, broj pogodenih ili potencijalno pogodenih korisnika;

Izmjena

(c) stvarno prouzročenu *materijalnu* ili *nematerijalnu* štetu ili *nastale* gubitke u mjeri u kojoj ih je moguće utvrditi. Pri evaluaciji tog aspekta u obzir se uzimaju, među ostalim, stvarni ili potencijalni finansijski ili gospodarski gubici, učinci na druge usluge, broj pogodenih ili potencijalno pogodenih korisnika;

Amandman 109

Prijedlog direktive

Članak 29. – stavak 7. – točka ca (nova)

Tekst koji je predložila Komisija

Izmjena

(ca) sve relevantne prethodne povrede koje je počinio dotični subjekt;

Amandman 110

Prijedlog direktive

Članak 29. – stavak 7. – točka cb (nova)

Tekst koji je predložila Komisija

Izmjena

(cb) načinu na koji je nadležno tijelo doznalo za kršenje, osobito je li i u kojoj mjeri subjekt obrade izvijestio o kršenju;

Amandman 111

Prijedlog direktive

Članak 29. – stavak 7. – točka g

Tekst koji je predložila Komisija

Izmjena

(g) razinu suradnje *fizičkih ili pravnih osoba koje se smatraju odgovornima* s nadležnim tijelima.

(g) razinu suradnje s nadležnim tijelima *kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja*;

Amandman 112

Prijedlog direktive

Članak 29. – stavak 7. – točka ga (nova)

Tekst koji je predložila Komisija

Izmjena

(ga) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su finansijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

Amandman 113

Prijedlog direktive

Članak 29. – stavak 9.

Tekst koji je predložila Komisija

Izmjena

9. Države članice osiguravaju da

9. Države članice osiguravaju da

njihova nadležna tijela obavješćuju relevantna nadležna tijela ***predmetne države članice*** imenovana u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] pri izvršavanju svojih nadzornih i provedbenih ovlasti kojima je cilj osigurati da ključni subjekt koji je identificiran kao kritičan ili kao subjekt istovjetan kritičnom subjektu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] ispunjava obveze u skladu s ovom Direktivom. Na zahtjev nadležnih tijela iz Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata], nadležna tijela mogu izvršavati svoje nadzorne i provedbene ovlasti nad ključnim subjektom koji je utvrđen kao kritičan ili istovjetan kritičnom subjektu.

njihova nadležna tijela ***u stvarnom vremenu*** obavješćuju relevantna nadležna tijela ***svih država članica*** imenovana u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] pri izvršavanju svojih nadzornih i provedbenih ovlasti kojima je cilj osigurati da ključni subjekt koji je identificiran kao kritičan ili kao subjekt istovjetan kritičnom subjektu u skladu s Direktivom (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata] ispunjava obveze u skladu s ovom Direktivom. Na zahtjev nadležnih tijela iz Direktive (EU) XXXX/XXXX [Direktiva o otpornosti kritičnih subjekata], nadležna tijela mogu izvršavati svoje nadzorne i provedbene ovlasti nad ključnim subjektom koji je utvrđen kao kritičan ili istovjetan kritičnom subjektu.

Amandman 114

Prijedlog direktive Članak 30. – stavak 4. – točka g

Tekst koji je predložila Komisija

(g) naložiti tim subjektima da objave aspekte nepoštovanja obveza predviđenih ovom Direktivom na utvrđeni način;

Izmjena

Briše se.

Amandman 115

Prijedlog direktive Članak 30. – stavak 4. – točka h

Tekst koji je predložila Komisija

(h) objaviti izjavu u kojoj se navode pravne ***i fizičke*** osobe odgovorne za povredu obveze utvrđene u ovoj Direktivi i priroda te povrede;

Izmjena

h) objaviti izjavu u kojoj se navode pravne osobe odgovorne za povredu obveze utvrđene u ovoj Direktivi i priroda te povrede;

Amandman 116

Prijedlog direktive Članak 31. – stavak 2.

Tekst koji je predložila Komisija

2. Upravne novčane kazne izriču se uz mjere iz članka 29. stavka 4. točaka od (a) do (i), članka 29. stavka 5. i članka 30. stavka 4. točaka od (a) do (h) ili umjesto njih, ovisno o okolnostima svakog pojedinog slučaja.

Izmjena

(Ne odnosi se na hrvatsku verziju.)

Amandman 117

Prijedlog direktive Članak 31. – stavak 3.

Tekst koji je predložila Komisija

3. **Pri odlučivanju** o izricanju upravne novčane kazne *i* o njezinu iznosu dužna se pažnja u svakom pojedinom slučaju posvećuje barem elementima predviđenima u članku 29. stavku 7.

Izmjena

3. **Odlučivanje** o izricanju upravne novčane kazne *ovisi o okolnostima svakog pojedinog slučaja, a pri odlučivanju* o njezinu iznosu dužna se pažnja u svakom pojedinom slučaju posvećuje barem elementima predviđenima u članku 29. stavku 7.

Amandman 118

Prijedlog direktive Članak 32. – stavak 1.

Tekst koji je predložila Komisija

1. Ako nadležna tijela imaju naznake da povreda obveza utvrđenih u člancima 18. i 20. koju je počinio ključni ili važni subjekt obuhvaća povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se obavještuje u skladu s člankom 33. te uredbe, ***u razumnom*** roku obavješćuju nadzorna tijela nadležna u skladu s člancima 55. i 56. te uredbe.

Izmjena

1. Ako nadležna tijela imaju naznake da povreda obveza utvrđenih u člancima 18. i 20. koju je počinio ključni ili važni subjekt obuhvaća povredu osobnih podataka iz članka 4. stavka 12. Uredbe (EU) 2016/679 o kojoj se obavještuje u skladu s člankom 33. te uredbe, ***bez nepotrebne odgode, a svakom slučaju u roku od 24 sata,*** obavješćuju nadzorna tijela nadležna u skladu s člancima 55. i 56.

te uredbe.

Amandman 119

Prijedlog direktive Članak 32. – stavak 3.

Tekst koji je predložila Komisija

3. Ako je nadzorno tijelo nadležno u skladu s Uredbom (EU) 2016/679 osnovano u državi članici drugačijoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo **može obavijestiti** nadzorno tijelo osnovano u istoj državi članici.

Izmjena

3. Ako je nadzorno tijelo nadležno u skladu s Uredbom (EU) 2016/679 osnovano u državi članici drugačijoj od one u kojoj je osnovano nadležno tijelo, nadležno tijelo **obavještava** nadzorno tijelo osnovano u istoj državi članici.

Amandman 120

Prijedlog direktive Članak 34.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 34.a

Odgovornost za nepoštovanje obveza

Ne dovodeći u pitanje bilo koji dostupan administrativni ili izvansudski pravni lijek, primatelji usluga koje pružaju ključni i važni subjekti, koji su prouzročili štetu zbog svoje neusklađenosti s ovom Direktivom, imaju pravo na učinkovit pravni lijek.

Amandman 121

Prijedlog direktive Članak 35. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

Komisija **periodično** preispituje funkcioniranje ove Direktive te podnosi izvješće Europskom parlamentu i Vijeću. U izvješću se posebno **ocjenjuje** relevantnost sektora, podsektora, veličine i vrste subjekata iz priloga I. i II. za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. U tu svrhu te u

Komisija **sake 3 godine** preispituje funkcioniranje ove Direktive te podnosi izvješće Europskom parlamentu i Vijeću. U izvješću se posebno **procjenjuje u kojoj je mjeri Direktiva doprinijela osiguravanju visoke zajedničke razine sigurnosti i cjelovitosti mrežnih i informacijskih sustava, istodobno**

cilju daljnog unapređivanja strateške i operativne suradnje, Komisija uzima u obzir izvješća skupine za suradnju i mreže CSIRT-ova o iskustvu stečenom na strateškoj i operativnoj razini. Prvo izvješće podnosi se do ...[**54** mjeseci od datuma stupanja na snagu ove Direktive].

pružajući optimalnu zaštitu privatnog života i osobnih podataka te relevantnost sektora, podsektora, veličine i vrste subjekata iz priloga I. i II. za funkcioniranje gospodarstva i društva u pogledu kibersigurnosti. U tu svrhu te u cilju daljnog unapređivanja strateške i operativne suradnje, Komisija uzima u obzir izvješća skupine za suradnju i mreže CSIRT-ova o iskustvu stečenom na strateškoj i operativnoj razini. Prvo izvješće podnosi se do ...[**36** mjeseci od datuma stupanja na snagu ove Direktive].

Amandman 122

Prijedlog direktive Prilog I. – točka 5. (Zdravlje) – alineja 6. (nova)

Tekst koji je predložila Komisija

Sektor	Podsektor	Vrsta subjekta
5. Zdravlje		<ul style="list-style-type: none">– pružatelji zdravstvene zaštite iz članka 3. točke (g) Direktive 2011/24/EU (90)– referentni laboratoriji EU-a iz članka 15. Uredbe XXXX/XXXX o ozbiljnim prekograničnim prijetnjama zdravlju⁹¹– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova iz članka 1. točke 2. Direktive 2001/83/EZ⁹²– subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. NACE Rev. 2– subjekti koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja („popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“) iz članka 20. Uredbe XXXX⁹³

⁹¹ [Uredba Europskog parlamenta i Vijeća o ozbiljnim prekograničnim prijetnjama zdravlju i stavljanju izvan snage Odluke br. 1082/2013/EU, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 727 final.]

⁹² Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001. o zakoniku Zajednice o lijekovima za humanu primjenu (SL L 311, 28.11.2001., str. 67.).

⁹³ [Uredba Europskog parlamenta i Vijeća o jačanju uloge Europske agencije za lijekove u

pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 725 final.]

Izmjena

Sektor	Podsektor	Vrsta subjekta
5. Zdravlje		<ul style="list-style-type: none">– pružatelji zdravstvene zaštite iz članka 3. točke (g) Direktive 2011/24/EU ⁹⁰– referentni laboratorijski EU-a iz članka 15. Uredbe XXXX/XXXX o ozbiljnim prekograničnim prijetnjama zdravlju⁹¹– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova iz članka 1. točke 2. Direktive 2001/83/EZ ⁹²– subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. NACE Rev. 2– subjekti koji proizvode medicinske proizvode koji se smatraju ključnim tijekom izvanrednog stanja u području javnog zdravlja („popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“) iz članka 20. Uredbe XXXX ⁹³– <i>subjekti koji imaju odobrenje za distribuciju iz članka 79. Direktive 2001/83/EZ</i>

⁹¹ [Uredba Europskog parlamenta i Vijeća o ozbiljnim prekograničnim prijetnjama zdravlju i stavljanju izvan snage Odluke br. 1082/2013/EU, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 727 final.]

⁹² Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001. o zakoniku Zajednice o lijekovima za humanu primjenu (SL L 311, 28.11.2001., str. 67.).

⁹³ [Uredba Europskog parlamenta i Vijeća o jačanju uloge Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda, upućivanje će se ažurirati nakon donošenja prijedloga COM(2020) 725 final.]

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Mjere za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanje izvan snage Direktive (EU) 2016/1148		
Referentni dokumenti	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)		
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 21.1.2021		
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	LIBE 21.1.2021		
Pridruženi odbori - datum objave na plenarnoj sjednici	20.5.2021		
Izvjestitelj(ica) za mišljenje Datum imenovanja	Lukas Mandl 12.4.2021		
Razmatranje u odboru	16.6.2021	3.9.2021	11.10.2021
Datum usvajanja	12.10.2021		
Rezultat konačnog glasovanja	+: -: 0:	44 14 4	
Zastupnici nazočni na konačnom glasovanju	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rares Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in 't Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Proccaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vronidi, Jadwiga Wiśniewska, Javier Zarzalejos		
Zamjenici nazočni na konačnom glasovanju	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh		

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani